DHS Transition Issue Paper

Big Data

OVERVIEW - ***Generating Value from DHS Data – Making DHS Data a Strategic Asset***

- The Department of Homeland Security (DHS) is working to make its data a strategic asset for the homeland security enterprise. Following two years of the Unity of Effort policy, both headquarters and mission component leaders are increasingly prepared to integrate data management into their normal business and decision making. The DHS Data Strategy will provide a foundation of enterprise data management values, guidelines, and principles. However, the full potential of DHS enterprise data management will not be realized without decisive leadership and investment from the next administration. With leadership and resource support, DHS will be able to leverage its data assets to create added value in five (5) major areas:

Mission

Risk-based priorities requiring enterprise-wide data management including, but not limited to: screening and vetting, threat assessment, and distribution of assets for preparedness, response and recovery. Early successes have been achieved in this area through leading projects like the DHS Data Framework for the Homeland Security Intelligence Enterprise, DHS Office of Policy's Immigration Data Integration Initiative, and S&T Homeland Security Advanced Research Projects Agency's (HSARPA) Data Analytics Engine (DA-E).

Management

Enterprise priorities for understanding, organizing, analyzing and making management decisions. Early success in this area has already been seen with the Management Directorate's Management Cube, an innovative solution that brings together essential management data to enhance decisions and performance.

Planning

Supporting and driving DHS strategic planning by using enterprise data management to support risk assessment, resource allocation, and performance assessment.

Research

Rapid evaluation of emerging big data and advanced computational techniques that are relevant to significantly improving the leveraging of DHS data, and prioritized delivery of enterprise services. HSARPA's DA-E works across industry, academia and government to understand rapid technical innovations that create opportunities and risks for homeland security mission.

Enterprise Service Delivery

The DHS OCIO, with Component partners, plays a lead role in delivering enterprise services for data management.

Course of action:

Leadership and Priorities	Enterprise data management shall be governed under the Information Sharing and Safeguarding Governance Board (ISSGB) and establish a network of component-level Chief Data Officers (CDOs), to be coordinated under the oversight of the ISSGB.
Policy Standards and Enforcement	DHS shall define and enforce policy standards for enterprise data management.

Compliance	The Department must ensure that it complies with all legal and policy requirements in the maintenance collection, storage, use, dissemination, archival and disposal of its data (e.g., Privacy Act of 1974, 5 U.S.C. § 552a).
R&D	S&T leads the Department's efforts to innovate and evaluate emerging big data solutions and related technologies to provide technical guidance, consultation and potential solutions for missions of Homeland Security Enterprise.
Enterprise Technology Development	DHS carefully develops, leverages and deploys efficient technologies to meet current data management needs. The DHS OCIO, with Component partners, will play a key role in delivering enterprise services for data management.
Communications	DHS effectively communicates, and understands, the value of data management, from not only leadership, but from operators, analysts and planners who know what they need from our DHS data.

DETAILED DISCUSSION

- As the DHS Data Strategy directs, DHS Enterprise Data Management must be directly tied to our strategic, mission priorities as a Department.
- The FY2017-2021 DHS Data Strategy provides a foundational set of principles and guidelines that can be used to efficiently drive data management.
- DHS S&T works directly with industry, academia and other government organizations to challenge, understand, leverage and adapt rapidly changing technologies to meet homeland security mission needs such as self-service data, virtualized data collection, point and click data wrangling, geo-coding, entity resolution, social media analytics, real-time intelligent systems and automated reporting in a manner that is consistent with legal authorities and privacy, civil rights, and civil liberties policies, and adequate intellectual property rights.
- The DHS OCIO works directly with all members of the homeland security enterprise to capture prioritized, mission requirements for data management, and then, leveraging the groundbreaking research and development of S&T, partners with the enterprise to deliver essential services and platforms.

Issue Background

- DHS manages significant data holdings across a broad set of missions and activities, many of which are public facing and occur in a rapidly evolving threat environment. With the establishment of the Department in 2002, each of its legacy Components retained ownership and management of its own data, often with decentralized data systems supporting the various operational missions of DHS.
- As such, DHS data is complex and must be managed appropriately. This includes ensuring that the Department protects the privacy, civil rights and civil liberties of individuals whose information we maintain. This also includes ensuring that the Department obtains adequate intellectual property rights to meet its missions.
- Current data management challenges and gaps include, but are not limited to:
  - ➢ Keeping pace with enterprise wide, cross component, mission needs;
  - ➢ Different policies on how to maintain what is otherwise similar data.
  - ➢ Development of intelligence insights from multiple transactional screening systems;

  - Analysis and reporting of immigration and other statistics across multiple immigration and other data systems that are not necessarily linked;
  - Strengthening and maturing the oversight of DHS finances and spending; and
  - Bottlenecks in hiring of human capital resources to address operational gaps.
- In order to provide strategic value to the homeland security enterprise over the next four (4) years, DHS will need to operationalize the principles of the DHS Data Strategy, focusing on strategic priorities for Mission, Management, and Planning.

Course of Action – Moving from Data Management Principles to Data Management Execution

Leadership, Governance and Priorities	First and foremost, we need a way to set our data management priorities to link our business and mission needs to our data needs. In practice, this means establishing a DHS enterprise-wide management role that is operated at the highest levels of the Department. This entity will listen to the real-world needs of our operators, our analysts, our managers, and our planners, and obtain decisions on the priorities from our Department senior leadership. Further, it will ensure that DHS has the agility and flexibility to apply its limited resources on a prioritized, risk-informed basis. This oversight should be led by the Information Sharing and Safeguarding Executive and supported by a network of component level Data Officers, in turn supported by a network of data scientists and managers.
Policy Standards & Enforcement	Second, DHS must set and enforce pragmatic data and data science policy standards that efficiently create manageable network effects across DHS strategic data sources. These standards will make it easier for data owners to adopt and lead to improved accessibility for authorized use at the scale demanded by homeland security applications.
Compliance	Third, we need to ensure that Department-wide, our enterprise data management priorities, methodologies, uses and implementation controls are in line with legal authorities, and, privacy, records management, civil rights and civil liberties laws and policies, and adequate intellectual property rights.
R&D	Fourth, technology evolves at a rapid pace requiring that DHS quickly assess and understand both opportunities and threats that emerge from new capabilities. DHS S&T hosts an internal Data Analytics Engine (DA-E) laboratory where DHS components and the Homeland Security Enterprise can examine the impact of emerging technology on current and future missions. This consolidated research and development activity makes experimentation, prototyping and piloting of technology efficient in a manner where lessons learned and best practices can be easily shared across homeland security organizations.
Enterprise Service Delivery	Fifth, the DHS OCIO manages a series of enterprise services and platforms which, in direct partnership with DHS components, actively seek out and deliver on the prioritized requirements of the homeland security enterprise for mission-based data management solutions.
Communications	Sixth, we need clear communication of priority technical, policy and management directions to DHS executives, managers, and most

	importantly analysts, responders, and operators to effectively implement enterprise data management

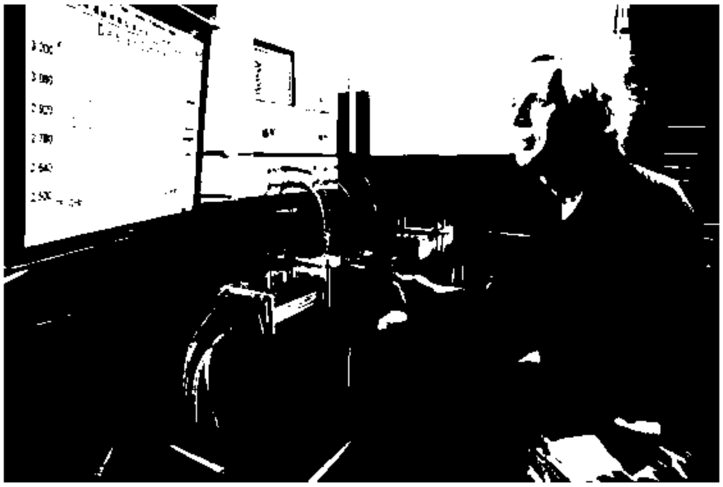
Major Risks ***What Happens if We Don't Make Data a Strategic Asset at DHS?***

- DHS risks generating huge inefficiencies, and associated financial costs, in how data are collected, shared, transferred, and used, with components creating their own, walled off data management solutions.
- DHS risks using data in inappropriate and illegal ways.
- DHS risks not achieving our actual mission and obligations to the American people by failing to identify and mitigate a security threat, missing a vital lead or a critical link, or failing to deploy an essential asset. Without rapid assessment and deployment of technology, DHS systems can quickly become ineffective against sophisticated threats.

Key Partnerships

- Intelligence Community
- Other Federal agencies
- State, Local, Tribal, Territorial stakeholders
- International partners
- Non-Governmental Organizations
- Public / Private agencies
- Data Analytics and Advanced Computing Industry
- Computer Science, Engineering, Math and Science Academic Organizations

Science and Technology



The Science and Technology Directorate is the primary research and development arm of the Department. It provides federal, state and local officials with the technology and capabilities to protect the homeland.

The Under Secretary for Science and Technology acts as the principal science and technology advisor to the Secretary and his/her Cabinet.

S&T has resident scientific expertise and capabilities in the following domains including, but not limited to:

- Situational Awareness and Decision Support Engine (SANDS)
- Communications & Networking Engine (CNET)
- Data Analytics Engine (DAE)
- Identity & Access Management Engine (IDAM)
- Behavioral, Economic & Social Sciences Engine (BESSE)
- Modeling & Simulation Engine (MSE)
- Manufacturing Engine (MANE)
- Mission & Operational Systems Analysis
- Test and Evaluation
- Application of Standards
- Systems Engineering & Transition
- Human Systems Integration
- Architecture Engineering
- Technology Foraging & OpEx
- Tech Transfer & Commercialization
- Partnership Coordination
- Sponsored R&D
- Intellectual Property Management

S&T owns and operates national laboratories which perform research and scientific and forensic analysis. S&T works with the broader R&D community to identify and adapt existing R&D investments to meet operator needs and challenges in four general areas:

- Technological capabilities for addressing DHS operational and strategic needs or that are necessary to address evolving homeland security threats.
- Systems-based analysis for introducing streamlined, resource-saving process improvements and efficiencies to existing operations.
- Improvements for enabling more effective and efficient operations and avoiding costly acquisition failures and delays by leveraging S&T's technical expertise to improve project management, operational analysis and acquisition management.
- Opportunities for collaboration across departmental, interagency, state and local and international boundaries to advance knowledge and understanding of existing and emerging threats and help identify a path forward.

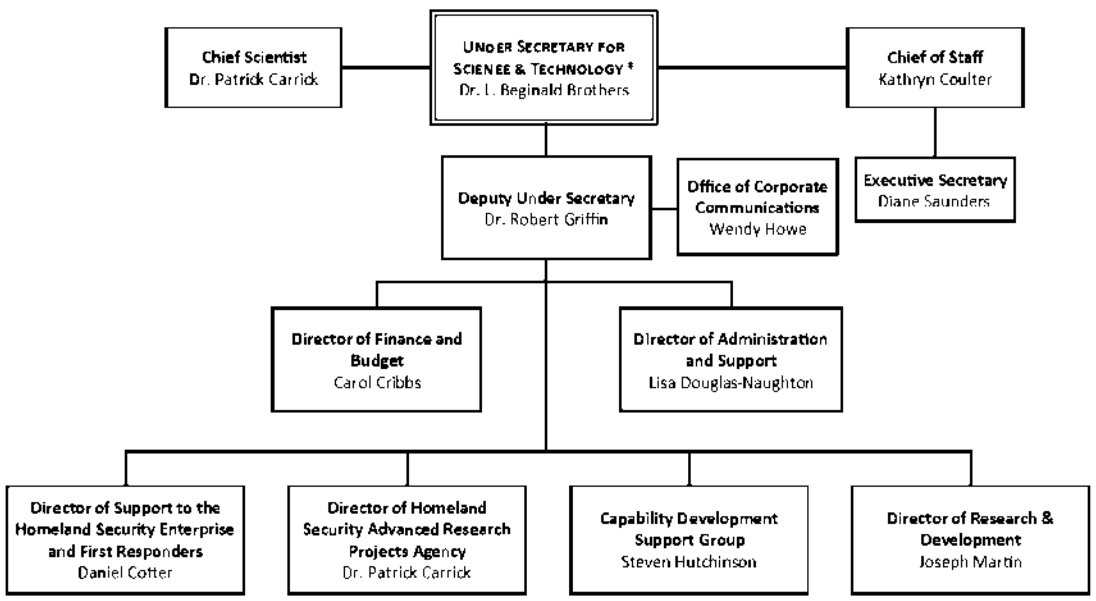
From border security and biological defense to cybersecurity and explosives detection, S&T is at the forefront of integrating R&D across the public and private sectors and the international community. By working directly with responders and component partners across the nation, S&T strives to provide advanced capabilities and analytics to better prevent, respond to and recover from the major threats to homeland security.

Mission

S&T's mission is to deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise.

Organization Chart

Science & Technology Directorate


UNDER SECRETARY FOR SCIENEE & TECHNOLOGY *
Dr. L. Reginald Brothers
Chief Scientist
Dr. Patrick Carrick
Chief of Staff
Kathryn Coulter
Executive Secretary
Diane Saunders
Deputy Under Secretary
Dr. Robert Griffin
Office of Corporate Communications
Wendy Howe
Director of Finance and Budget
Carol Cribbs
Director of Administration and Support
Lisa Douglas-Naughton
Director of Support to the Homeland Security Enterprise and First Responders
Daniel Cotter
Director of Homeland Security Advanced Research Projects Agency
Dr. Patrick Carrick
Capability Development Support Group
Steven Hutchinson
Director of Research & Development
Joseph Martin

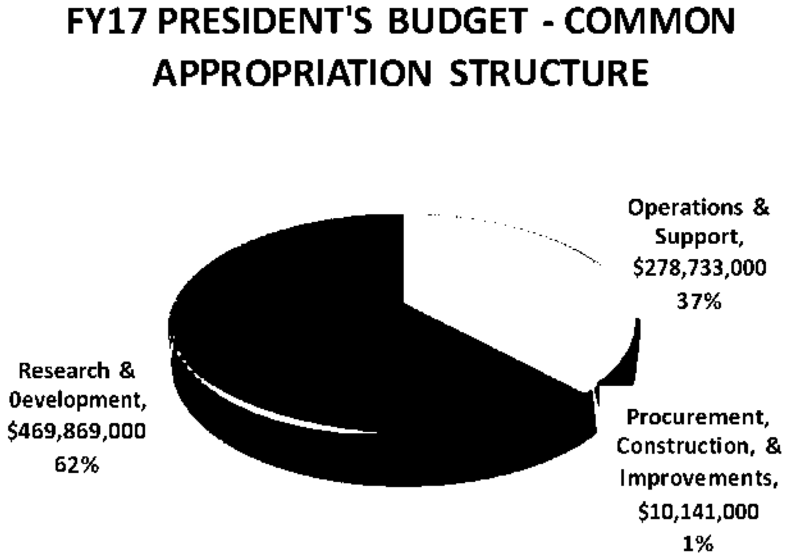
Key

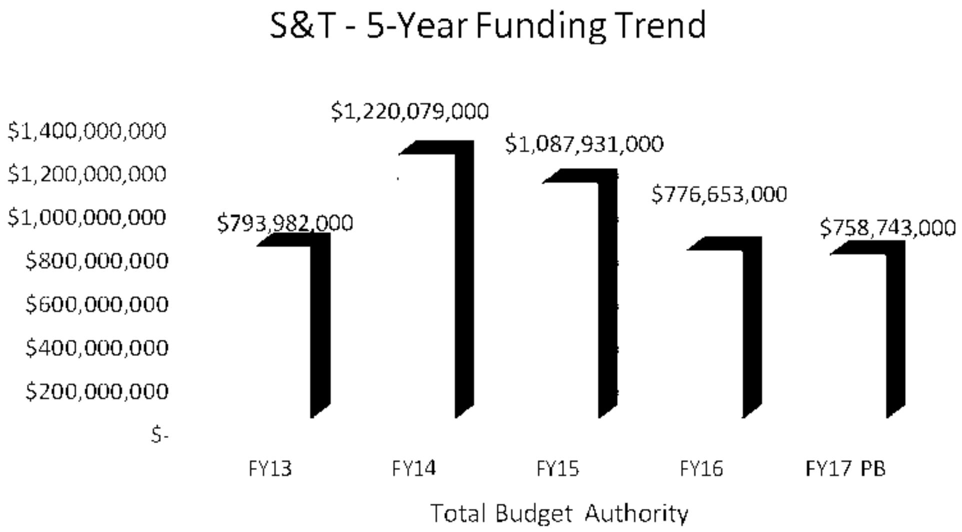
* Senate Confirmed	** Reports to OGC
Non-Career	Career
Acting Non-Career	Acting Career
Non-Career or Career Position	

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to~~ information, and civil and/or criminal fines and penalties.

Budget

Total Budget Authority		
[redacted]	[redacted]	[redacted]
$776,653,000	$758,743,000	-17,910,000





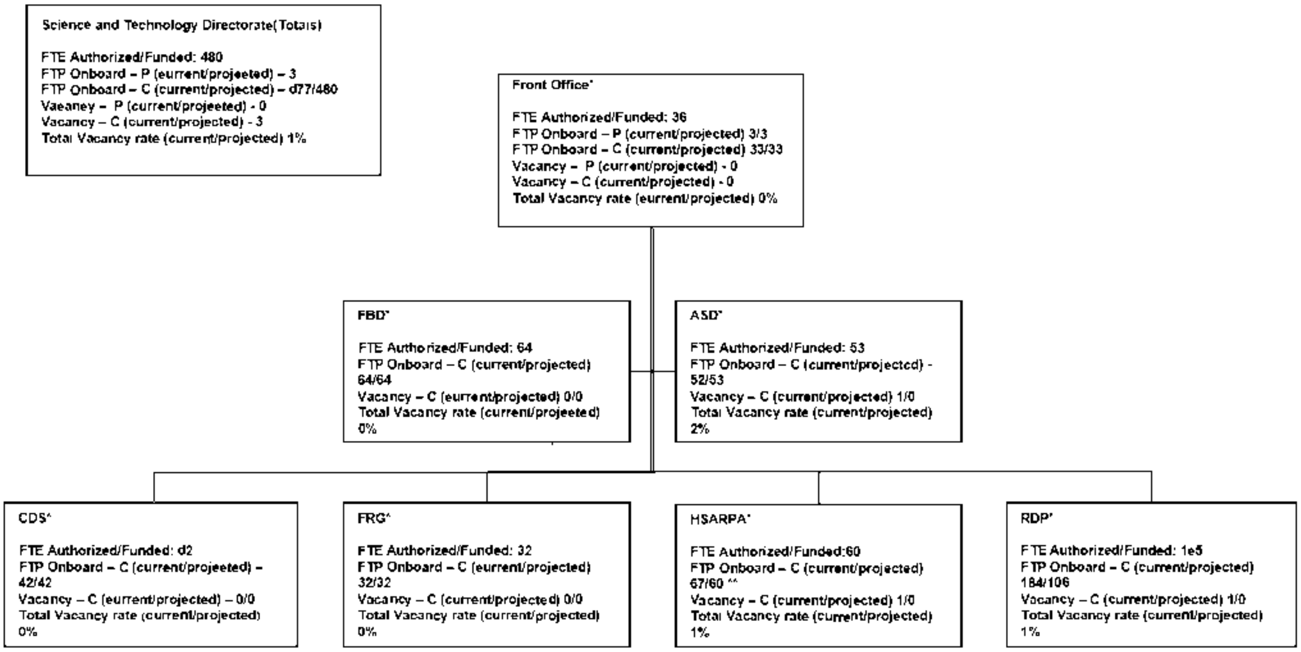
~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

Workforce

[redacted]	[redacted]	[redacted]
480	477	3 / 1%

* FY 2016. Does not include reimbursable, working capital, or revolving account employees

Workforce Chart



Science and Technology Directorate(Totals)

FTE Authorized/Funded: 480
FTP Onboard – P (eurrent/projeeted) – 3
FTP Onboard – C (current/projected) – d77/480
Vaeaney – P (current/projeeted) - 0
Vacancy – C (current/projected) - 3
Total Vacancy rate (current/projected) 1%

Front Office*

FTE Authorized/Funded: 36
FTP Onboard – P (current/projected) 3/3
FTP Onboard – C (current/projected) 33/33
Vacancy – P (current/projected) - 0
Vacancy – C (current/projected) - 0
Total Vacancy rate (eurrent/projected) 0%

FBD*

FTE Authorized/Funded: 64
FTP Onboard – C (current/projected) 64/64
Vacancy – C (eurrent/projected) 0/0
Total Vacancy rate (current/projeeted) 0%

ASD*

FTE Authorized/Funded: 53
FTP Onboard – C (current/projectcd) - 52/53
Vacancy – C (current/projected) 1/0
Total Vacancy rate (current/projected) 2%

CDS*

FTE Authorized/Funded: d2
FTP Onboard – C (current/projeeted) – 42/42
Vacancy – C (eurrent/projected) – 0/0
Total Vacancy rate (current/projected) 0%

FRG*

FTE Authorized/Funded: 32
FTP Onboard – C (eurrent/projected) 32/32
Vacancy – C (current/projected) 0/0
Total Vacancy rate (current/projected) 0%

HSARPA*

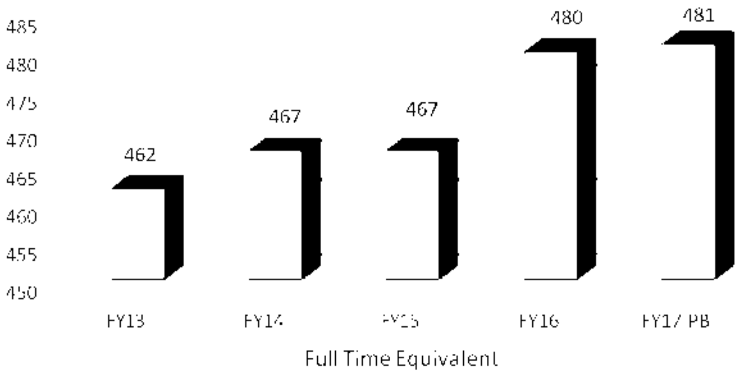
FTE Authorized/Funded:60
FTP Onboard – C (current/projected) 67/60 **
Vacancy – C (current/projected) 1/0
Total Vacancy rate (current/projected) 1%

RDP*

FTE Authorized/Funded: 1e5
FTP Onboard – C (current/projected) 184/106
Vacancy – C (current/projected) 1/0
Total Vacancy rate (current/projected) 1%

NOTES
- * There are no set number of authorized positions by group
- ** Projection may change if CBRNE transfer does not occur (4 FTEs)

S&T - 5-Year Workforce Trend



~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

Strategic Priorities

- **DHS R&D Coordination and Prioritization through Integrated Product Teams (IPTs):** With increased, complex threats, in an austere fiscal environment, we must be strategic about our R&D work and how we prioritize our investments. The IPT process, managed by S&T and staffed by the components, will improve acquisition across DHS by identifying technological capability gaps and coordinating R&D to close those gaps across the Department's mission areas. Through an integrated investment process, S&T will explicitly tie its investments to specific areas, including: Presidential-national, Departmental, and other priorities as they arise.

- **Advancing Cyber & IT Security:** Cyber adversaries have presented a full spectrum of threats not only to the U.S. government, but also to private organizations and critical infrastructure sectors. All systems must be protected, and have processes in place to obtain and implement upgrades in real-time to secure mission-critical systems. S&T partners with national and international leaders in cyber security to leverage our resources and capabilities for optimal results.

- **Keeping Pace with Technology:** Government's ability to discover and implement new technologies is commonly outpaced by adversaries and the private sector. Processes for acquisition and security, for example, are typically not designed to keep up with the rapid pace of technology, leaving little choice but to manage unaddressed threats with inadequate, last-generation tools. Through S&T's technology foraging, operational experimentation, unique partnerships, research and development agreements between governments and the private sector, prize challenges, accelerators and public outreach, we are better positioned to address gaps in capabilities by mobilizing the Homeland Security Industrial Base.

- **Energize the Homeland Security Industrial Base in support of providing leading, cutting-edge solutions to operational Components and first responders.** Because DHS has largely utilized commercially available, off-the-shelf products to achieve its mission, partnership with industry is essential. We are striving to create a private sector community around homeland security challenges that sees the DHS mission as a joint mission. The use of prize challenges, accelerators, public outreach and other vehicles has generated significant interest in the private sector in being part of a Homeland Security Industrial Base.

- **Support technology assessments for all major acquisitions in the Department to ensure technical maturity:** S&T conducts a systems engineering review and technology assessment of the technical solutions in DHS major acquisition programs and provides a report to the Chief Acquisition Officer and Joint Requirements Council prior to the decision to enter the "Obtain" phase of the Acquisition Life Cycle. Integrated with the IPTs, this ensures that S&T is involved early in the acquisition process to assess the technical maturity of the technologies that DHS major acquisitions intend to acquire. S&T is poised to play a larger role in this mission space.

- **Integrating Technology as an Element of Change to all Risk and Threat Calculations:** All risk and threat calculations take current or next-generation technologies into account, yet few run the same calculations on potential future threats. By doing this, we can keep up with threats but not get ahead of what is to come. S&T will look to provide this future view through supporting technological risk assessments of Technology Readiness Levels 3, 4, 5, and more generations down the road.

- **Instilling a Homeland Security Enterprise Approach since Threats Know No Borders**: Today's threats come in all shapes and sizes, yet none are restricted by borders. Therefore, detecting and managing these threats must be done in partnerships that cross government entities, state/local/federal jurisdictions, and international borders. S&T scouts opportunities to build solutions directly with the operational front lines of homeland security.

- **Establish the future National Bio- and Agro-Defense Facility (NBAF), and its supporting enterprise-wide ecosystem, as the leading biocontainment facility for the study of foreign animal and emerging zoonotic diseases that threaten animal agriculture and public health in the United States:** The first laboratory facility in the United States of its kind, this $1.2 billion facility will allow researchers to study zoonotic diseases that affect livestock and other large animals. In preparation for its completion in 2022, S&T is focusing on construction of the 570,000 square-foot biocontainment facility with leading-edge capabilities and security; transition planning of operations from the Plum Island Animal Disease Center (PIADC) in New York; and the creation of an ecosystem that attracts partners and fosters innovation to tackle the biggest threats facing our animal agriculture.

- **Shape a Workforce Culture Specifically Formulated for R&D:** A workforce specifically focused on R&D is composed of very different attributes than that of operational organizations. Achieving the required skills, mindset, and balance/composition of the team are all critical to its success. S&T will craft a workforce plan and build its workforce by continuously reviewing and mining data to inform hiring and development investments in the near term, and yield the right mix of knowledge, skills and capabilities over the long term that will be necessary to accomplish our R&D mission.

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

Key Partnerships/Stakeholders

Interagency	
Partner	**Description**
Interagency Relationships	S&T partners with many agencies across government to support its missions operating laboratories and Centers of Excellence, interfacing with the intelligence community, identifying capability gaps and requirements, and supporting test & evaluation in areas such as explosives, Counter-*Unmanned* Aerial Vehicles, and First Responders.

Stakeholder Groups and Federal Advisory Committees (FACA)	
Partner	**Description**
S&T's Homeland Security Science & Technology Advisory Committee	S&T manages its own FACA compliant advisory committee that is comprised of citizens from academia, the private sector, and former governmental officials. The USST utilizes the HSSTAC to assist in bringing in new opinions and ideas to foster the best effectiveness and direction of the Directorate.
Stakeholder Groups	S&T partners with multiple stakeholder groups in various topic areas such as first responders, communications, preparedness, explosives, and intelligence. These partnerships are helpful to identify requirements, assess needs and capability gaps, conduct operational field assessments, and collaborate with the larger community.

Industry / Public-Private / Academia	
Partner Name	**Description**
Academic Institutions	S&T establishes and manages the DHS Centers of Excellence and partners with other academic institutions in support of projects and programs such as Small Unmanned Aerial Systems.
Industry Relationships	S&T partners with industry for technology transition, conducting pilots, developing technologies, supporting the Transportation Security Laboratory and many important programs and projects within the Directorate.

International Engagements	
Partner	**Description**
International Agreements/Relationships	S&T works with many countries via bilateral and other agreements to leverage international resources in the science and technology, and research and development community.

Legislative Priorities

- **Other Transactional Authority (OTA).** Currently, OTA is set to expire with the end of the Fiscal Year on September 30, 2016. In the past, it has been renewed via the annual appropriations bill. S&T leadership has been working with authorizing committees to insert language that would extend OTA by five years and provide stability for the programs that use it.

- **Personnel Hiring.** Section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105 261) provides for a special hiring authority for agencies to bring onboard personnel with highly specialized and leadership backgrounds for select positions. Currently, per the Homeland Security Act of 2002, this authority resides with the HSARPA Director. S&T is seeking legislation which would move that authority to the Under Secretary for Science and Technology.

- **Integrated Product Teams (IPTs).** At the direction of Secretary Johnson, the IPTs were re-instituted by Under Secretary Brothers as a way for S&T to assist operational components with determining their technology requirements and planning for the long-term implementation of technological solutions. S&T is seeking legislation that would specifically call out the IPTs to ensure the long-term viability of this critical mechanism.

- **R&D Funding.** By nature, R&D necessitates different funding structures than infrastructure. For successful R&D programs to truly deliver disruptive, impactful products for operators, they must be funded with an eye toward consistency over the term of development. Infrastructure, on the other hand, is funded annually and can be managed as such. Therefore, S&T is seeking to earn an understanding that R&D funding needs to be separated from infrastructure funding so the very different needs of each can be applied.

- **National Bio and Agro Defense Facility (NBAF).** Due to the heavy investment which USDA is making in the agricultural threat, DHS and USDA have begun preliminary discussions as to which agency should manage the NBAF once it becomes operational. Although S&T is not seeking any legislative action at this time, the Senate mark up of both the DHS and Agriculture Appropriations Bills included language for S&T and USDA to have these discussions.

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

Government Accountability Office / Office of the Inspector General Audits

GAO Audits		
Title	**Description**	**Final Report Due**
Microbial Forensics: DHS and FBI Biological Attribution Capabilities (Engagement Code 460639)	Objective to answer the following questions: (1) How have the DHS and FBI assessed the technical and scientific needs for attribution of a biological attack since 2010? (2) What scientific and technical gaps remain, if any, in DHS and FBI capabilities to attribute the source of a biological attack, including an attack using a novel synthetic biological weapon?	11/15/2016
Multiplex Point-of-Care Technology (Engagement Code 100311)	The committees seek to do an assessment of multiplex point-of-care technology (POCT) to address the following: (1) Has your agency funded work to develop or test such technologies, and if so, at what stage of development or testing is the technology, and what are the known performance characteristics (for example, sensitivity, specificity, and limits of detection) of the technology? (2) What is known about the performance characteristics of multiplex POCT in the industrial sector? (3) What technical issues are associated with multiplexing assays used in such technology? (4) What are the known benefits, costs, and implementation challenges of this technology?	4/10/2017

OIG Audits		
Title	**Description**	**Final Report Due**
Review of the DHS Science and Technology Directorate's Efforts to Protect Information Systems from Insider Threats OIG Project No. 15-107-ITA-S&T	The objective is to determine the current risk by assessing the effectiveness of steps S&T has taken to protect its IT assets and data from potential unauthorized access, disclosure, or misuse by its employees, contractors, and business partners especially those with special or elevated access based upon their job descriptions or functions.	Audit On Hold as of 10/21/2015

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

DHS Transition Issue Paper
Research and Development Profile

OVERVIEW

- Many of the Department of Homeland Security's (DHS) 240,000 employees are on the front lines addressing border and maritime security, immigration, disaster response, or protecting the nation's leadership. The Department also provides support for its vast homeland security network at the state, local, and tribal levels. As such, the DHS research and development (R&D) profile is modeled to serve this customer base with solutions that link directly to their technological needs.
- DHS has three entities appropriated to conduct R&D: the U.S. Coast Guard (USCG), the Domestic Nuclear Detection Office (DNDO), and the DHS Science and Technology Directorate (S&T).[1]
- S&T coordinates R&D efforts across the Homeland Security Enterprise (HSE), which includes DHS Components and others with a homeland security mission.
- USCG conducts research across all eleven USCG statutory mission areas. This includes joint research, development, and testing with the Department of Defense (DoD).
- DNDO focuses its R&D on national detection and forensics technologies and capabilities for nuclear and radioactive materials.
- DHS works closely with Components to transition solutions into the field through a coordinated R&D approach that best serves DHS and the HSE.
- The Under Secretary for S&T serves as the science advisor for the Secretary to provide guidance on current and emerging threats and provides mitigation strategies.
- The Director of DNDO advises the Secretary regarding R&D efforts and priorities related to radiological and nuclear detection and countermeasures in support of the Department's missions.
- S&T contributes to the Unity of Effort by coordinating R&D across the Department to inform a wise investment strategy and realize efficiencies across Components.

DETAILED DISCUSSION

Role of DHS in R&D

Within DHS, R&D is predominantly performed by the Science and Technology Directorate, the U.S. Coast Guard, and the Domestic Nuclear Detection Office. USCG and DNDO have specific mission areas of focus while S&T maintains a broader scope of R&D to support the Department and HSE at large, which can include the private sector and first responders who also have a stake in homeland security. As the mission space is vast across DHS and the HSE, S&T, USCG, and

[1] Beginning in FY2017, additional Components and Directorates will have R&D funding under the Common Appropriation Structure (CAS). These include the Transportation Security Administration, National Protection & Programs Directorate, United States Secret Service, and the Under Secretary for Management. Reforms under the CAS have resulted in greater transparency of R&D activities that are occurring within other Components as part of acquisition programs. Because these projects are smaller scale and more targeted, they are not included for discussion in this paper.

DNDO have focused attention on core areas in order to provide R&D for the highest priorities as well as emerging threat areas as they arise.

Organization	R&D Focus Areas
Science and Technology Directorate	• Borders and Maritime Security
	• Critical Infrastructure and Resilience
	• Counterterrorism
	• Countering Violent Extremism
	• Cybersecurity
	• Mass Transit Security
	• Big Data
	• First Responders
	• Explosives Detection
	• Chemical and Biological Security
	• Emerging Homeland Security Threats
U.S. Coast Guard	• Ports, Waterways, and Coastal Security
	• Drug Interdiction
	• Aids to Navigation
	• Search and Rescue
	• Living Marine Resources
	• Marine Safety
	• Defense Readiness
	• Migrant Interdiction
	• Marine Environmental Protection
	• Ice Dperations
	• Maritime Law Enforcement
DNDO	• Cost-effective equipment to ensure widespread deployment
	• Detection of heavily-shielded special nuclear material
	• Enhanced wide-area monitoring and search
	• Monitoring challenging pathways
	• Nuclear forensics signatures of interdicted material

The DHS Science and Technology Directorate (S&T) was established by Congress in 2003 to deliver effective and innovative insight, methods, and solutions for the critical needs of the HSE.

S&T facilitates and supports its R&D process through its four groups.

- First Responders Group (FRG) identifies, validates, and facilitates the fulfillment of first responder capability gaps through the use of existing and emerging technologies, knowledge products, and the acceleration of standards. FRG manages working groups, teams, and other stakeholder outreach efforts to better understand the needs and requirements of state, local, tribal, and federal first responders, including those on the front lines of border protection and transportation security.

- Homeland Security Advanced Research Projects Agency (HSARPA) works with all DHS Components to understand and address their high-priority R&D requirements and operational needs through the analyses of current missions, systems, and processes. HSARPA's goal is to integrate knowledge, technologies, and science-based solutions into the DHS enterprise.

- Capability Development Support Group (CDS) instills the rigor and analysis needed to make smart investment decisions that deliver enhanced capabilities to HSE operators. It focuses on capability-based assessments, operations analysis, risk management, standards, systems engineering, the systems engineering life cycle (SELC), SELC tailoring, and test and evaluation.
- Research and Development Partnerships Group (RDP) provides the HSE with access to science-based capabilities and solutions through a vast network of trusted partnerships, and manages instrumental tools that sponsor critical research and development activities. RDP forges partnerships with five primary advanced research communities that include the private sector, academia, national laboratories, other departments and agencies, and international partners.

S&T has shaped its portfolio around operator, Department, and Executive Branch needs, while positioning itself to provide rapid response to emerging threats that occur in the ever-evolving security landscape. DHS has galvanized a network of partners that are essential for expanding R&D investments and finding next generation solutions that could solve homeland security challenges quicker or at a lower cost to the government. By leveraging traditional and non-traditional partnerships, the end goal is to find near-term, incremental solutions while continuing to research longer-term goals.

In recent years, S&T has implemented new programs and initiatives that address longstanding needs outlined in statute and by the Government Accountability Office. The new approach applies focus to the Directorate's R&D portfolio, while also finding increased inroads into Components to accurately gather needs and requirements. Furthermore, S&T has adopted a rigorous approach to review its R&D programs. With new processes in place and strengthened relationships among DHS Components, the Directorate looks to continue its role of delivering solutions to the front lines.

Visionary Goals

To focus its portfolio, S&T developed Visionary Goals that map to the Quadrennial Homeland Security Review and Executive Branch priorities. The visionary goals are set for 20 to 30 years, and are a vector for the organization to work toward. This model recognizes that reaching these goals will take time and a suite of solutions, including both technologies and knowledge products. The goals are:

- Responder of the Future: Protected, Connected, and Fully Aware
- Resilient Communities: Disaster-Proofing Society
- Enable the Decision Maker: Actionable Information at the Speed of Thought
- Trusted Cyber Future: Protecting Privacy, Commerce, and Community
- Screening at Speed: Security that Matches the Pace of Life

To support the Visionary Goals, S&T has developed programs that address issues in the short term and bring together core capabilities to deliver solutions on an accelerated schedule. Identified as Apex programs and engines, they are designed to provide solutions into the mission space within a short amount of time. For example, the Apex Border Enhancement Analytics Program, which utilized the core capabilities from the Apex Data Analytics Engine, delivered a tool to Immigration and Customs Enforcement to enhance their weapons counter-proliferation investigation capabilities. S&T delivered the tool in approximately three years.

Given the constantly evolving security landscape, S&T also understands that it needs to be prepared to take on rapid response projects. In addition to its core focus areas, S&T stands ready to support the Secretary and the Executive Branch to address emerging needs. In recent years, S&T has assisted the Secretary and the administration in addressing non-traditional aviation technology, smart gun technology, social media analytics, and countering violent extremism in response to national events.

The United States Coast Guard (USCG) Research, Development, Test and Evaluation (RDT&E) Program conducts research to support all eleven of the USCG's statutory mission areas. This includes joint research, development, and testing with DoD.

- The mission of the USCG RDT&E Program is to provide innovative technologies, premier analysis, and decision support to enhance operational performance, develop new capabilities, inform the acquisition process, and reduce risk across the vast USCG mission space both as a part of the HSE and as a Military Service. As a military service, the USCG provides a vital link to DoD and other military R&D programs and services.
- The USCG Research and Development Center (RDC), located in New London, CT, is the project execution and demonstration laboratory for the CG. It houses the Joint DHS and USCG S&T Innovation Center, and the Modeling & Simulation Center-of-Excellence. The RDC also oversees the Joint Maritime Test Facility with Naval Research Lab in Mobile, Alabama, for conducting full-scale ship fire safety and oil spill response technology testing.

The Domestic Nuclear Detection Office (DNDO) focuses its R&D on national detection and forensics technologies and capabilities for nuclear and radioactive materials.

- DNDO continues to develop breakthrough technologies that increase performance and reduce the operational burdens of our frontline operators and improve their mission performance.
- DNDO works closely with U.S. Customs and Borders Protection (CBP), USCG, TSA, and state and local partners to identify key operational requirements for the design of next-generation nuclear detection devices that can be used by law enforcement and technical experts during operations.
- DNDO also advances fundamental knowledge in nuclear detection and forensics through a sustained long-term investment in basic and applied research as well as academic research supporting the next generation of scientist and engineers.

Conducting R&D for the Department of Homeland Security

In August 2015, the Secretary requested that an IPT Process be instituted to ensure the highest R&D priorities were being addressed through a process focused on Components, while fostering collaborative efforts and capabilities regarding research and development. The IPTs are aligned to the Department's core missions as identified in the Quadrennial Homeland Security Review. They represent mission-focused teams of Component operators and DHS technical experts in key threat areas. The IPT Process is a unity of effort initiative that empowers the Department to make sound R&D investments. These decisions are based on a plan that comes directly from the Component front lines and is informed by technical experts. This is also intended to de-conflict duplicative efforts.

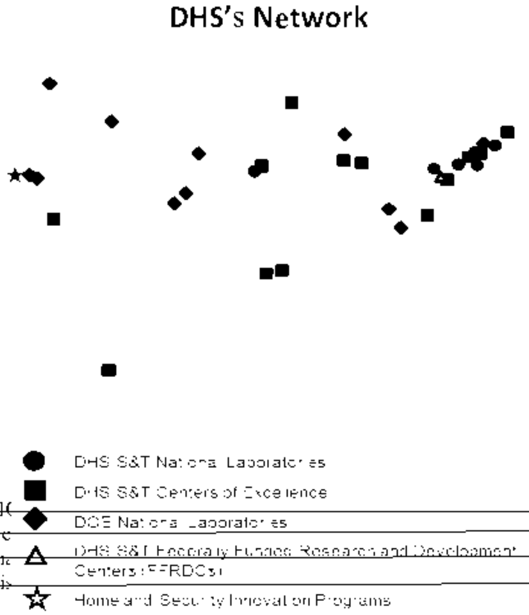
While S&T oversees the overall effort, the specific IPTs are led by operational Components, with subject matter experts from DHS headquarters participating as members. Together, they identify capability gaps to gain a better understanding of current and emerging needs at DHS Components. For example, FRG is a part of this process through its own IPT, the First Responder Resource Group (FRRG). The FRRG is comprised of State, Local, Tribal and Territorial first responders and emergency management personnel from across the nation. Its findings are published to industry, academia, and the HSE. The IPTs are also fed by other processes such as the Joint Requirements Council (JRC).

The JRC is chartered by the Secretary as a Component-composed, Component-chaired council to develop and lead the Department's Component-driven joint operational requirements process. It oversees and manages the Department's process to generate, validate and prioritize capability needs through the establishment and management of functionally-aligned portfolio structures. This oversight includes prioritization of joint operational requirements, as well as mandating joint development of requirements documentation. The JRC also supports and informs the DHS IPT Process with JRC-collected operational capability gaps containing technology or R&D needs. The JRC and IPTs serve as the mechanisms for identifying, prioritizing, and addressing operational capability and technological capability gaps, respectively.

A Network of Partnerships

DHS depends on a vast network of partnerships and is building new relationships with creative problem solvers such as start-ups, incubators, and accelerators. DHS leverages these networks to convene experts, demonstrate technologies, find emerging solutions, and commercialize technologies. This network includes:

- Five DHS laboratories and as many as 13 Department of Energy national laboratories;
- Ten Centers of Excellence that extend to a consortium of hundreds of universities;
- Direct grants to over 30 universities;


DHS's Network
● DHS S&T National Laboratories
■ DHS S&T Centers of Excellence
◆ DOE National Laboratories
△ DHS S&T Federally Funded Research and Development Centers (FFRDCs)
☆ Homeland Security Innovation Programs

- Contracts with nearly 30 companies;
- 13 international partners;
- Other federal departments and agencies and Federally Funded R&D Centers; and
- Homeland Security Innovation Programs in premier regional hubs for innovation.

Courses of Action

With a balanced portfolio and improved processes in place, DHS looks to execute its strategic vision to provide solutions for the most pressing homeland security problems. To achieve this, DHS will strengthen relationships within the Department and expand valuable partnerships externally to more rapidly meet homeland security needs. As the R&D organizations for homeland security and its operators, DHS S&T, DNDO, and USCG will play multi-faceted roles that continue to evolve as the security landscape changes. Specifically, potential courses of action include:

1. Adjust the DHS R&D budget to more robustly address operational and capability gaps.
2. Establish a funding mechanism to address unforeseen threats so investments in current projects can come to fruition.
3. Decrease the variability year-to-year in R&D funding so investments in current projects can come to fruition.
4. Advance the work of the JRC and IPTs by supporting and further institutionalizing their work as a strong policy of the Department.
5. Maintain a status quo of all R&D efforts and budget.

#149 - Please provide a list of all S&T personnel in international positions, where they are located, and the associated costs.

Response: S&T Personnel in International Position: S&T Attaché, U.S. Embassy London

Associated Costs: $345,000

- International Cooperative Administrative Support Services (ICASS) - $90,000.
  This is paid to embassy for all shared services such as security guards, normal-hour motorpool, routine health visits, phone operators, printing, etc.
- Capital Security Cost Sharing (CSCS) Program (Annual Costs) - $50,000
  This is for cost sharing across DHS for all personnel posted overseas.
- London Housing- $80,000
  This is housing for the detailee in London.
- London Locally Employed Staff (LES) - $85,000
  This is for a full-time employee that works for ICPO at the London Embassy Office.
- London Miscellaneous – $40,000
  This is for the detailee's housing bills (i.e. Water, Gas, Electric) as well as the London office IT, Shipping, Over-time Motorpool, etc.

#150 - Please provide final FY 2016 measures of effectiveness used by S&T's senior leadership team along with any weekly/monthly/quarterly updates throughout the year.

Response: The Portfolio Analysis and Review (PAR) for the Science and Technology Directorate (S&T) has been used to support strategic decision making regarding the health of the S&T investment portfolio. This is the process by which S&T measures metrics, technical merits, program execution, and strategy moving forward. PAR along with the standard efforts examining budget and human resources is just one of the tools used to establish a baseline where yearly evaluations are made. The FY 2016 data were captured in the areas of metrics and measures, program gaps, alignment to goals, risk, and milestones. The FY 2016 results revealed that a number of programs at S&T needed to improve the metrics to ensure measurability and alignment. The data were used to work with all projects to improve metrics and measures, such that now 95 percent of the R&D programs have solid metrics. This improvement helps to ensure that our programs/projects have measurable performance outputs, outcomes, and eventually impacts. FY 2016 is a step forward in insuring coverage of the vast majority of S&T's investments and forms a good baseline for measuring overall program/project health. Through this effort S&T measures the degree to which its programs/projects are successful.

A quantified answer to each of the following questions was computed for each of the R&D programs in FY16. This assessment directly impacted program execution and an updated assessment is underway for FY17.

- Is the portfolio aligned with our customer's mission?
- Is our R&D investment positioning the organization for the future?
- Are we sufficiently innovative in the way we approach our challenges?
- Are we working with the right partners and leveraging external resources?
- Are we clear on what we are trying to achieve and using measurable performance parameters to track outcomes?
- Are we transitioning relevant products to the field?
- Do we have a consensus on the health of the program/project?

Lastly, in addition to programmatic measures, human capital and financial execution measures of effectiveness are also critical for S&T leadership to monitor.

PAR data updates, which includes programmatic and financial execution measures, are collected quarterly from all S&T investments. PAR quarterly data is compiled, analyzed, and the results are reported to leadership. PAR results inform leadership's strategic program decisions and supply content for weekly reports to the Office of the Under Secretary of S&T. All PAR data and reports including these measures of effectiveness are pre-decisional and For Official Use Only (FOUO), and therefore are not externally releasable.

The newly established Research, Development, and Innovation (RD&I) Process is expanding on the strategic PAR process to ensure all investment types get appropriate oversight at the strategic and tactical levels. The updated RD&I process is led by the Executive Steering Council and includes group-level and division-level regular reviews of programmatic and technical progress. The result of the process is a performance based budget and strategically aligned plan for executing the resources appropriated to S&T, as well as a prioritized list of unfunded programs and other support functions. This prioritization is captured in an S&T Integrated and Prioritized Project List which is submitted to the Under Secretary of Science and Technology for approval and used to formulate budgets and develop annual execution and spend plans. This procedure links the policies and processes needed to integrate Directorate R&D planning, execution, and budget cycles.

#151 - Please provide a copy of S&Ts 2016 and 2017 strategic plans, including all progress and status updates.

Response: The S&T directorate released a visionary strategic plan in 2015 to describe the mission and approach for 2015-2019. S&T has been focused on its implementation since its publication.

S&T's annual Portfolio Analysis and Review (PAR) process collects and analyzes data from all R&D, non-R&D, and R&D infrastructure investments to allow leadership to evaluate the strategic direction. The findings and recommendations from the PAR and other leadership oversight activities result in portfolio adjustments, but maintain consistency with the direction provided in the published Strategic Plan.

On June 8, 2016, the Office of the Chief Scientist (OCS) led the annual PAR Strategic Review, which included Group-level presentations of their updated strategic plans. Additionally, a strategic discussion was facilitated where key questions were discussed and next step directions were given. A few examples of the strategic discussion points are as follows:

1. Of the total DHS R&D budget, what is the appropriate fraction of investments to make in projects that could fundamentally change the nature of a capability and create opportunities that have unprecedented impact (high-risk/high-payoff)? Must these be aligned with the IPTs?
    - OCS was tasked with conducting this study. A growth horizon model was used to evaluate best practices from other private sector and public sector organizations. An analysis of what the split of S&T's current portfolio is underway.
2. The natural investment dollar "churn rate" where projects come to an end (e.g., go/no-go Key Performance Parameters, natural, etc.) and the funding is up for reinvestment in new projects starts appears to be low at the project level. What is the appropriate percentage of S&T's funding that is available for project-level new starts each year?
    - OCS was tasked with conducting this study. An initial version was conducted at the program level. Additional work is required to get a higher fidelity result.
3. What is the appropriate fraction of the S&T projects that should have independent Test and Evaluation (T&E) (by $ and/or by #)? Or, what is the appropriate criteria? Should a responsible party (e.g. Developmental Testing and Evaluation Office within the Capability Development Support Group or OCS) be asked to certify all S&T's T&E results for 100% of the projects and prioritize projects for third party T&E?
    - An RD&I process, overseen by S&T's Executive Steering Committee (ESC), has been established to address this issue. The portfolio has been split into three categories based on the yearly budget. The level of review appropriate to each investment level is currently being defined by the ESC.

All the updates to the strategic review currently contain For Official Use Only / Pre-Decisional information.

The Directorate has continued in its strategic planning with Group-level strategic plan development. These plans are currently being drafted and will form the basis of a holistic update to the formal Strategic Plan during 2017. The Office of the Chief Scientist has been directed to lead this integrated update for DHS S&T, which will incorporate the Group-level plans, results from the PAR, and Integrated Product Teams (IPTs) guidance.

Attachment 1: S&T FY15 Strategic Plan

#156 - Please provide the number of SAFETY Act applications processed over the last 3 years and the average processing time.

Response: The number of SAFETY Act applications processed over the last 3 years and the average processing time are as follows:

FY 14 101 received, 65 approved, 119 days average processing time
FY 15 106 received, 87 approved, 110 days average processing time
FY 16 144 received, 76 approved, 117 days average processing time

Please note: Evaluations of applications received during the last 3-4 months of each FY are normally completed during the first part of the following FY. For example, at the end of FY16, 41 of the 144 applications filed during FY16 were still under review. The primary remaining difference between applications filed and those approved are applications that are determined to be incomplete, need further work, and then are resubmitted.

#157 - Regarding the IPTs, What is the process used to engage the whole Homeland Security Enterprise (HSE) (including state and locals)? What priorities have been established by the operational components, HSE?

Response: The IPT Process gains input from the state, locals, and tribal organizations by engaging first responders at all levels. This is accomplished by the R-Tech - First Responder Resource Group (FRRG) - which serves as a mechanism for continuous dialogue and the coordination of research, development, and delivery of technology solutions to first responders at the federal, state, local, tribal, and territorial levels. The FRRG is comprised of over 100 fire, emergency medical service, emergency management, and law enforcement first responders. The members provide personal insight into the unique requirements and needs of their cities, states, and regions. The FRRG helps to identify, validate, and facilitate the fulfillment of first responder needs through the use of existing and emerging technologies, knowledge products, and standards. The group meets annually in person and virtually throughout the year. The FRRG members are responsible for identifying and prioritizing the criticality of multiple capability gaps drawn from the DHS *Project Responder 4* report and defining the requirements associated with each potential technology solution. *Project Responder 4* identified gaps between current emergency response capabilities and those capabilities required to respond to a catastrophic incident. The input from the FRRG is helping S&T's First Responder Group align funding to address the highest priority needs of responders at all levels of government.

The primary goals of the FY17 Integrated Product Team (IPT) Process is to identify and prioritize research and development (R&D) technological capability gaps within the core missions of the Homeland Security Enterprise and coordinate DHS research and development efforts to close those gaps. The objectives for the FY17 IPTs are also consistent with IPTs strategic alignment, as follows:

- Ensure the Department is investing in non-duplicative R&D efforts to develop solutions that address the highest-priority technological capability gaps.
- Enhance the mechanisms that result in the Department's *High-Priority Technology Solutions* document – including the continued refinement of metrics to transition technology solutions and improve mission capabilities.
- Continue to develop and refine DHS acquisition and funding profiles and align them to the highest-priority gaps.
- Provide a standardized data collection and reporting process to capture all ongoing R&D activities that constitute the DHS-wide R&D profile.

The entire Homeland Security Enterprise is incorporated into the IPT process through a series of Sub-IPTs (32 in FY-17 managed at the DHS component level) that consist of DHS and non-DHS participants (FBI, National Institute of Standards and Technology, U.S. Navy, etc.) depending on the IPT mission space. These Sub-IPTs meet and determine the highest priority R&D gaps that may prevent a high profile or high risk project/program from achieving its objective.

The Sub-IPTs submit their input to the IPTs (DHS Leadership level) who refine the input to the top ten items. In FY17 a total of 64 gaps were submitted to the Senior Research Council, which consists of Senior DHS leaders who vote on the highest priorities for the Department. This resulted in 16 items to be reviewed and researched for solutions. This is all-component driven and S&T-coordinated. The FY16 IPT Report is attached; the FY 17 Report is due in January 2017.

IPTs include:

IPT Name	**Component IPT Chairs/Co-Chairs**	**Homeland Security Enterprise Membership**
Enhance Security	TSA	CBP, DHS HQ, FEMA, FPS, NCTC, TSA, USCIS, USSS, DNDO, NPPD Non-DHS: DoD, DOJ, DOT, FBI, White House CVE Task Force
Prevent Terrorism: CBRN	OHA	CBP, DHS HQ, S&T, DNDO, FEMA, OCHCO, OHA, TSA, USCG, USSS
Secure Borders	CBP	CBP, DHS HQ, ICE, S&T, USCG
Prevent Terrorism	I&A	CBP, CRCL, DHS HQ, DNDO, FEMA, I&A, ICE, NPPD, MGMT/OCIO, OGC/ILD, OPS, PLCY, TSA, USCG, USCIS
Secure Cyberspace	NPPD and MGMT/CISO	CBP, DHS HQ, S&T, FEMA, ICE, TSA, USCG, USCIS Non-DHS: NASA, DOJ, HHS
Incident Management	FEMA	CBP, DHS HQ, FEMA, ICE, NPPD, TSA, USCG, USSS, S&T State, Local, Tribal, and Territorial representation by DHS/FRRG

Attachment 3: FY16 IPT Report

Attachment 4: Project Responder 4 Report

Strategic Plan 2015–2019

Science and Technology Directorate

Homeland
Security

Science and Technology

MESSAGE FROM THE UNDER SECRETARY

The Science and Technology Directorate's (S&T) mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise. The successful execution of this mission rests significantly on whether we can transform our approach to research and development (R&D). This plan serves as the directorate's roadmap for how it plans to serve as a model for federal R&D.

In crafting this plan, I made four observations that I think are important to keep in mind as we implement this plan and pursue this goal. First, the Department of Homeland Security's operational and oversight responsibilities are enormous. As a department, we face complex operational threats and provide a range of solutions from tactical niche solutions to vast national-level capabilities. Second, I believe a balanced R&D portfolio teeming with innovative and force multiplying solutions is critical to ensuring the safety, security, and resilience of the homeland. Providing frontline operators with tools that secure them the upper hand in their respective environments is paramount. Third, S&T has a passionate and dedicated workforce. Walking the halls, I am invigorated by the widespread enthusiasm for our mission. Our workforce is hungry to contribute, and we have the technical expertise and depth to work hand-in-hand with operators and end users. Fourth, the federal government is no longer the majority provider of R&D funding, and we can no longer assume we have access to the best minds if we work exclusively through who and what we already know. To be a 21st-century R&D organization, we must tap innovation engines in the venture capital world, Silicon Valley, and universities. The more vehicles there are to work with those performers, the more effectively and efficiently S&T can develop security solutions.

To turn these observations into action we will look to this Strategic Plan and our five Visionary Goals—Screening At Speed, a Trusted Cyber Future, Enable the Decision Maker, Responder of the Future, and Resilient Communities—to guide our resource investments and unite our staff. These goals serve as our "North Star" and the basis for S&T's strategy. Equally important is how we deliver on these goals. We will choose projects strategically, ensuring they are force multipliers that address critical end-user needs and are aligned with the investments of our partner R&D organizations and industry. We will focus on energizing the Homeland Security Industrial Base to invest in future capabilities that will ensure the safety, security, and resilience of our nation. Finally, we will establish a strong and healthy leadership culture within the directorate.

I fully endorse the implementation of the *S&T Strategic Plan 2015-2019*.

Dr. Reginald Brothers
Under Secretary for Science and Technology
Department of Homeland Security

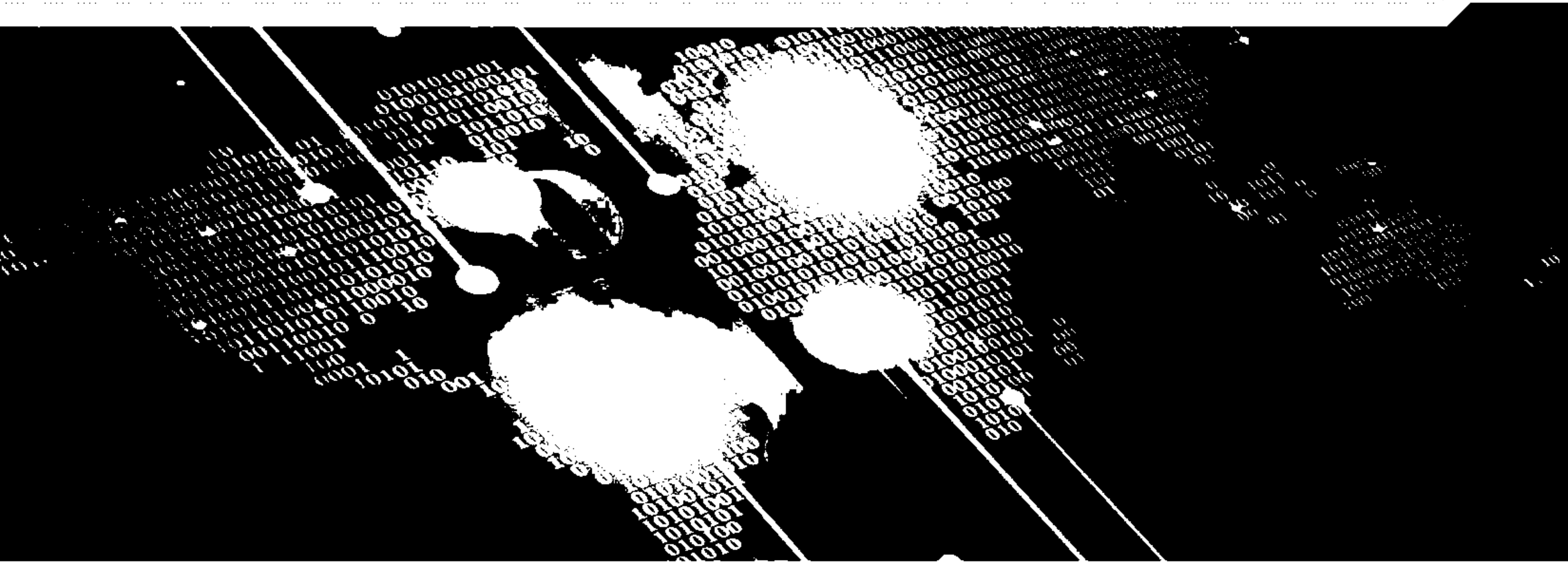
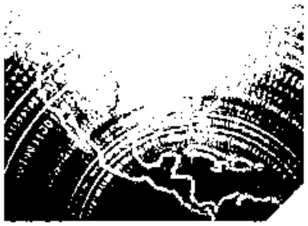


TABLE OF CONTENTS



EXECUTIVE SUMMARY

The Science and Technology Directorate (S&T) plays a critical role in addressing major homeland security threats for the Department of Homeland Security (DHS). S&T uses the knowledge of science and tools of technology to make our country, our communities, and our families more secure across the broad spectrum of threats facing the homeland—from counterterrorism to natural disasters. As the research and development (R&D) arm of DHS, S&T is responsible for leading R&D, demonstration, testing, and evaluation activities to ensure a safer, more secure nation.

S&T developed the *S&T Strategic Plan 2015–2019* to outline strategic objectives, initiatives, and activities for the next five years. Through the implementation of this plan and investment in a balanced portfolio of work, S&T will position the department to address the challenges of both today and tomorrow. Part I of this plan introduces the directorate and characterizes the strategic context it operates within. Part II of this strategic plan details the specific objectives, initiatives, and activities S&T will conduct in the next five years. Finally, Part III of this plan details S&T's R&D Capability Roadmaps, which will guide investments in the years to come.

PART I – Introduction and Strategic Context

S&T is one of a handful of DHS components created from whole cloth under the Homeland Security Act of 2002. In the last 12 years, the directorate has grown into a trusted partner for DHS operators and state, local, tribal, and territorial first responders. It is important to recognize that although R&D is the backbone of this organization, S&T maintains a diverse and complex set of roles and responsibilities that extend beyond a traditional R&D organization. These roles and responsibilities enable the directorate to serve as the glue between operational elements.

This strategic plan serves as the directorate's roadmap for how it will become a model for federal R&D. The plan's three strategic objectives were specifically designed to address the environment the directorate operates within today. Additionally, pursuant to guidance outlined in Secretary of Homeland Security Jeh Johnson's "Strengthening Departmental Unity of Effort" memo, the directorate established Visionary Goals. These goals will serve as 30-year horizon points to drive innovation within S&T and its ecosystem of technical expertise inside and outside of government.

EXECUTIVE SUMMARY CONTINUED

PART II – The Strategy

To keep pace with evolving threats and security challenges, S&T will implement several strategic objectives and initiatives. Through this work, S&T will ensure DHS is poised to bridge current capability gaps as well as anticipate homeland security challenges 20 to 30 years ahead.

The strategic plan details specific activities S&T will lead to achieve the objectives and initiatives laid out here:

Deliver Force Multiplying Solutions: S&T must focus its limited resources on delivering force multiplying solutions designed to address the highest priority needs. S&T's framework to achieve this objective involves the following interdependent initiatives:

Identify and Prioritize Operational Requirements and Capability Gaps – S&T actively participates in departmental and interagency governance bodies, as well as activities that enable direct engagement with operators, to identify and prioritize operational requirements and capability gaps.

Make Strategic Investments in High-impact, Priority Areas – The directorate's ability to make strategic investments in high impact, priority areas is dependent upon the cultivation of a balanced R&D portfolio and continued investment in national and directorate capabilities that enable R&D.

Partner with the Homeland Security Enterprise (HSE) – S&T must continuously invest in the creation and maintenance of partnerships with DHS components and other R&D organizations. Internal and external partnerships are a core element of our strategy and serve as the foundation of S&T's innovative ecosystem.

Energize the Homeland Security Industrial Base (HSIB): S&T will employ a robust array of tools to enhance private sector outreach, technology awareness, and R&D contracting. To achieve this objective, S&T will execute the following initiatives:

Optimize Markets by Pooling Demand and Developing Standards – S&T is working to integrate markets with international partners and to develop standards jointly with industry to better coordinate R&D investments, pool demand, and reduce costs.

EXECUTIVE SUMMARY CONTINUED

> *Engage the HSIB through a Deliberate, Continuous, and Transparent Approach – S&T will facilitate regular idea exchange between operational users and industry-based technologists by deploying new, non-traditional outreach mechanisms.*
>
> *Improve Programs Designed to Increase Collaboration with Innovative Companies – S&T will develop new approaches to engage non-traditional companies and revamp existing programs to become more timely and dynamic. Additionally, S&T will reengineer internal forecasting capabilities to better understand where to capitalize on industry investment trends.*

Establish a Strong and Healthy Leadership Culture: S&T's ability to achieve the aforementioned strategic objectives depends upon common identity, clarity of mission, and leadership at all levels of the organization. With empowerment, responsibility, and accountability as cultural values, S&T strives both to create an innovation-friendly environment and to give staff the tools and opportunities to grow and succeed within it. The following initiatives will enable S&T to fulfill this objective:

> *Empower the Workforce – S&T will give a stronger voice to staff and foster a broader sense of ownership and attachment to the organization and its direction. S&T values our workforce's perspective and believes that none of us individually is as smart as all of us collectively.*
>
> *Provide Meaningful Leadership Development and Professional Growth Opportunities – Diffusing leadership throughout S&T gives staff more input in and power over the direction of the organization. To make this possible, S&T will make targeted investments in tools and capabilities that ensure our workforce has the skills, competencies, and knowledge required to advance S&T's mission at all levels. S&T will further enable our staff by providing substantive training and workforce development opportunities.*
>
> *Engineer a Pipeline for the Next Generation of Homeland Security Professionals – To ensure that its future workforce sustains and builds on successes, S&T is committed to growing a pipeline for the next generation of staff. This two-part activity involves a continuous assessment of the organization that includes analyzing where staff needs will grow or decline and making long-term investments in growing areas to ensure that emerging workforce needs are addressed.*

PART III – S&T Research and Development Strategic Priorities

Each of S&T's five Homeland Security Advanced Research Projects Agency divisions, three First Responders Group divisions, and Apex programs and Technology Engines have developed Capability Roadmaps aligned to the needs of their operational end users. These high-level roadmaps formalize a vision, identify strategic drivers, provide future capability descriptions, and list R&D objectives for the next five years. In collaboration with HSE end users and HSIB partners, S&T's investment in projects aligned to these roadmaps will prepare the department for the challenges of both today and tomorrow.

INTRODUCTION AND STRATEGIC CONTEXT

Part I

INTRODUCTION AND STRATEGIC CONTEXT

The Science and Technology Directorate (S&T) is one of a handful of components in the Department of Homeland Security (DHS) created from whole cloth under the Homeland Security Act of 2002. In the last 12 years, the directorate has grown into a trusted partner for DHS operators and state, local, tribal, and territorial first responders. It is important to recognize that, although research and development (R&D) is the backbone of this organization, S&T maintains a diverse and complex set of roles and responsibilities that extend beyond a traditional R&D organization. These nontraditional R&D organization roles and responsibilities include, but are not limited to: (a) the coordination and administration of operational test and evaluation for all major DHS acquisitions; (b) the implementation of the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002; (c) in collaboration with the Office of the General Counsel, the management of the department's intellectual property portfolio; (d) in collaboration with all elements of DHS, the maintenance of the department's compliance with treaties such as the Biological Weapons Convention; and (e) the operation and maintenance of enduring national capabilities such as laboratories. These roles and responsibilities enable the directorate to serve as the glue between operational elements.

Through considerable work and dedication from its workforce, S&T has made the most of an industrial-age toolbox in a digital-age R&D landscape. This strategic plan serves as the directorate's roadmap for how it plans to serve as a model for federal R&D—hyper-connected, capable of meeting increasing demand for return on taxpayer dollars, and tailored to the digital age. The plan's three strategic objectives were specifically designed to address the strategic context of the environment the directorate operates within today.

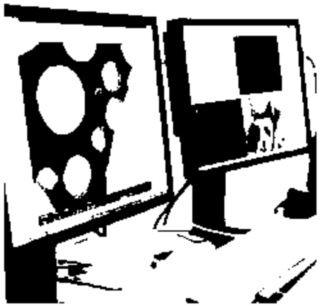
Given the current and projected threat environments, technology and R&D are the bridge to the future of homeland security. The most effective and efficient changes will come with the smart application of science and technical expertise to develop force multiplying solutions. These technology-based solutions will provide homeland security operators and first responders the upper hand in their respective operational spaces. They will also enable the Homeland Security Enterprise (HSE) to expand capabilities and security coverage, despite limited funds. Thus, the directorate's strategic objective to deliver force multiplying solutions is critical in the department's ability to fulfill its mission and operational demands.

HOMELAND SECURITY ENTERPRISE

Homeland security is a widely distributed and diverse national enterprise. The term enterprise refers to the collective efforts and shared responsibilities of those involved in maintaining critical homeland security capabilities. S&T considers the HSE and our international partners as our constituency—those we work with and for—to enhance our nation's security and resiliency.

DHS Components and Staff	**First Responders**
Federal Partnerships/the Interagency	**International Community**
Industry	**Academia**
Private Citizens	**Critical Infrastructure Owners and Operators**

S&T and the Homeland Security Industrial Base (HSIB) serve an enterprise that has a diverse set of needs, operates in a resource-constrained budget environment, conducts procurements in a sometimes fragmented way, and is often criticized for transparency and



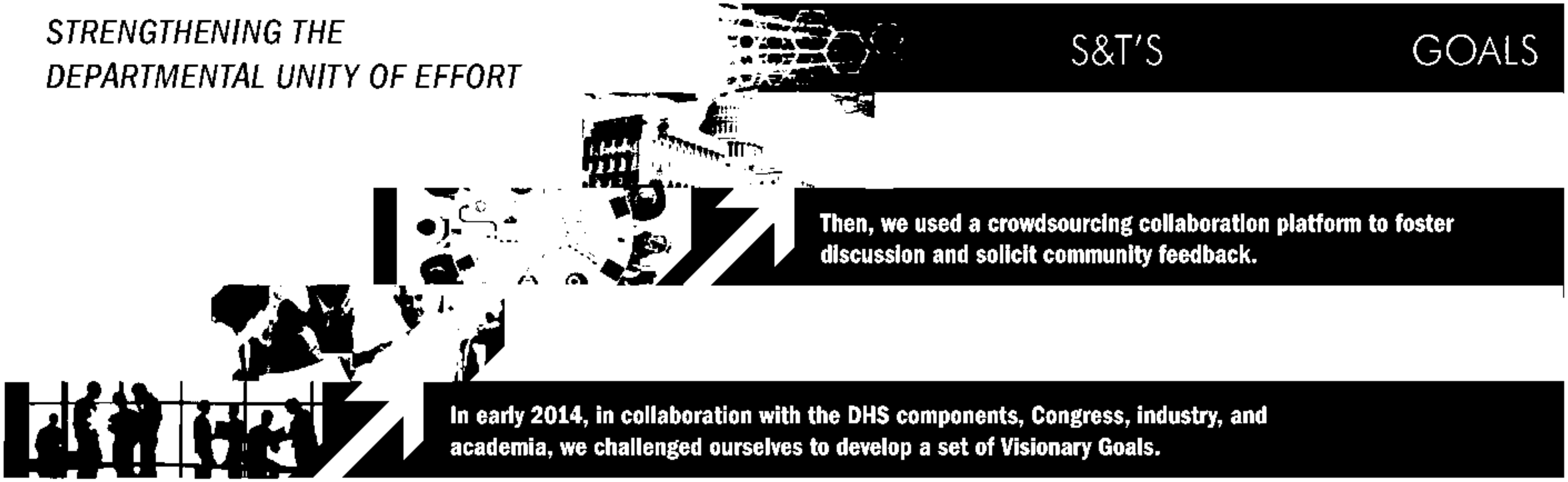
INTRODUCTION AND STRATEGIC CONTEXT CONTINUED

information sharing. These attributes are further complicated by the fact that technology evolution today outpaces federally funded R&D. Therefore, it is critical that S&T develops and sustains effective engagement with the HSIB to capitalize on externally funded investments and innovation. A private sector engine that is well-informed, incentivized, highly agile, and networked can better serve the HSE and improve the overall safety and security of the nation.

In order to achieve the directorate's mission, S&T must establish a strong and healthy leadership culture that recruits, develops, and empowers a 21st-century R&D workforce. To function in the new digital age, the directorate needs scientists who can break down firewalls and are fluent in the language of operators. These "multi-lingual" program managers must be empowered to make risk-informed decisions and manage a balanced R&D portfolio. To equip this workforce with the requisite skills, competencies, and knowledge to advance S&T's mission, the directorate must invest in tools, capabilities, training, and development opportunities.

Finally, it is important to highlight one additional element of S&T's strategic context. To effectively and efficiently address the range of challenges our nation faces, the department recently commenced an initiative entitled "Strengthening Departmental Unity of Effort." In this 2014 memorandum, Secretary of Homeland Security Jeh Johnson directed a series

STRENGTHENING THE DEPARTMENTAL UNITY OF EFFORT



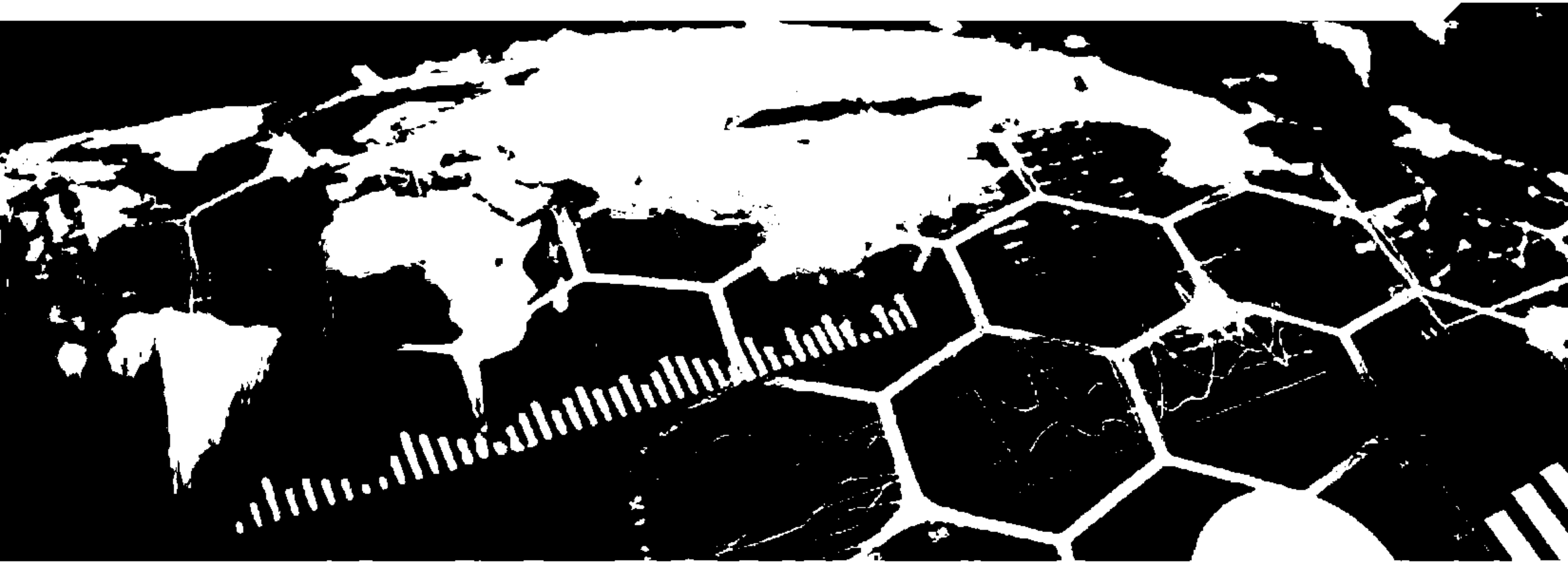
In early 2014, in collaboration with the DHS components, Congress, industry, and academia, we challenged ourselves to develop a set of Visionary Goals.

Then, we used a crowdsourcing collaboration platform to foster discussion and solicit community feedback.

S&T'S GOALS

of actions to create a more cohesive department while preserving the professionalism, skill, and dedication of the people within, as well as the rich history of the DHS components. Pursuant to this guidance, the directorate established Visionary Goals to better unify staff. The goals provide 30-year horizon points to drive innovation within S&T and its ecosystem of technical expertise inside and outside of government.

THE S&T STRATEGY



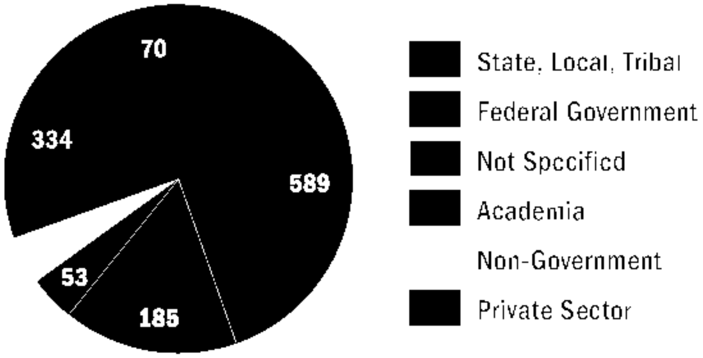
Part II

A MORE BALANCED APPROACH

S&T'S GOALS

In order to maximize unity of effort, S&T needed to create Visionary Goals that could unify the directorate and provide strategic direction for years to come. Before developing the Visionary Goals, S&T leaders agreed the goals must satisfy the following requirements: (a) align with DHS doctrine and policy; (b) address strategic challenges and threats prioritized by operators and end users in the HSE; and (c) inspire the science and technology ecosystem to collaborate on and invest limited resources in force multiplying solutions. With these requirements in mind, S&T launched an inclusive, transparent, and dynamic collaboration portal designed to facilitate the development of S&T's Visionary Goals. In the end, nearly 1,300 people within the HSE and HSIB contributed ideas.

BASIC MEMBER DATA
(1,298 Total Users)



Total Users

Votes 1,824

Ideas Posted 138

Comments 308

Users 1,298

A MORE BALANCED APPROACH CONTINUED

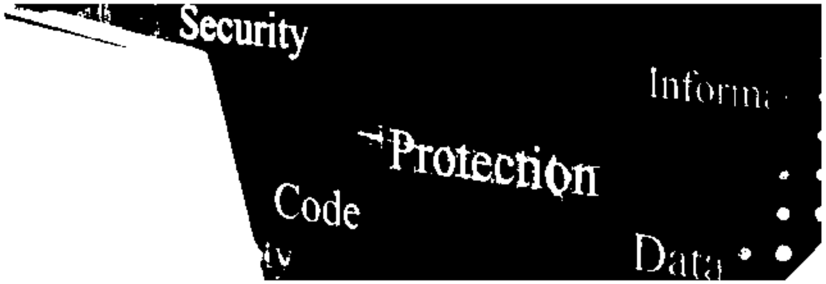
1990 FILM TOTAL RECALL STILL REPRODUCED WITH PERMISSION.

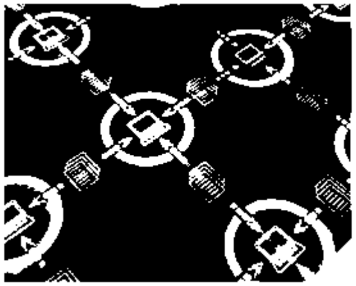
Based on input from S&T staff, stakeholders, and the public, S&T created the following Visionary Goals, which will serve as S&T's North Star:

REPRODUCED WITH PERMISSION FROM THE 1990 FILM TOTAL RECALL.

Screening At Speed: Security that Matches the Pace of Life

Noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Unobtrusive screening of people, baggage, or cargo will enable the seamless detection of threats while respecting privacy, with minimal impact to the pace of travel and speed of commerce.



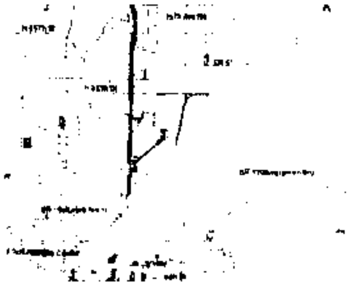


A Trusted Cyber Future: Protecting Privacy, Commerce, and Community

In a future of increasing cyber connections, underlying digital infrastructure will be self-detecting, self-protecting, and self-healing. Users will trust that information is protected, illegal use is deterred, and privacy is not compromised. Security will operate seamlessly in the background.

A MORE BALANCED APPROACH CONTINUED

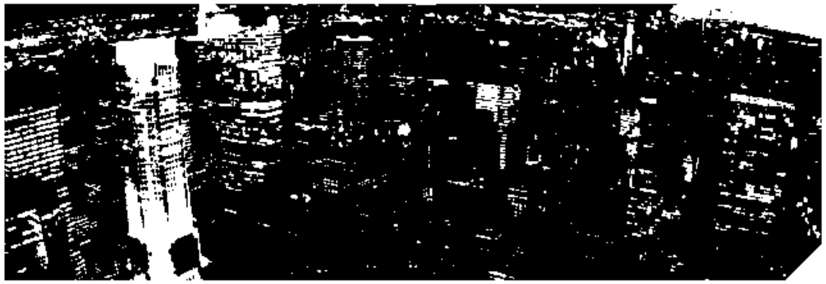
Enable the Decision Maker: Actionable Information at the Speed of Thought

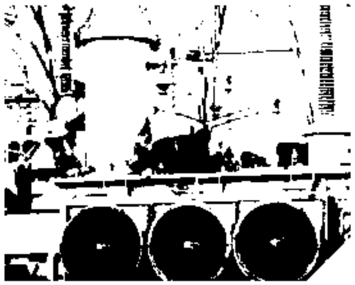


Predictive analytics, risk analysis, and modeling and simulation systems will enable critical and proactive decisions to be made based on the most relevant information, transforming data into actionable information. Even in the face of uncertain environments involving chemical, biological, radiological, or nuclear incidents, accurate, credible, and context-based information will empower the aware decision maker to take instant actions to improve critical outcomes.

Responder of the Future: Protected, Connected, and Fully Aware

The responder of the future is threat-adaptive and cross-functional. Armed with comprehensive physical protection, interoperable tools, and networked threat detection and mitigation capabilities, responders of the future will be better able to serve their communities.





Resilient Communities: Disaster-proofing Society

Critical infrastructure of the future will be designed, built, and maintained to withstand naturally occurring and man-made disasters. Decision makers will know when a disaster is coming, anticipate the effects, and use already-in-place or rapidly deployed countermeasures to shield communities from negative consequences. Resilient communities struck by disasters will not only bounce back, but bounce forward.

THE STRATEGIC FRAMEWORK

DELIVER FORCE MULTIPLYING SOLUTIONS

Given the operational demands on the department and the evolving landscape of threats and natural hazards, S&T must focus its limited resources on delivering force multiplying solutions designed to address the highest priority needs. S&T's framework to achieve this objective involves three interdependent initiatives: (a) identify and prioritize operational requirements and capability gaps; (b) make strategic investments in high-impact, priority areas; and (c) partner with the HSE to increase technology transition, reduce programmatic risk, and repurpose other agency investments. Each of these initiatives emphasizes more collaborative, active, and enduring partnerships with the HSE. By updating its approach to R&D, S&T will cultivate a highly relevant, diversified, and value-creating investment portfolio that delivers force multiplying solutions.

Identify and Prioritize Operational Requirements and Capability Gaps

No matter how big or small, the needs and ideas of the HSE are the seedlings of all current and future R&D at S&T. The directorate leverages numerous sources to collect these operational requirements and capability gaps. Employing a multi-pronged, expedient, and user-friendly approach, S&T actively participates in governance bodies and directly engages with operators. The resulting awareness and understanding of the HSE's operational needs allows S&T to identify cross-cutting requirements, set priorities, and make strategic investments. A few activities that exemplify this initiative include the following:

Departmental and Interagency Governance Bodies – The directorate participates in several standing executive steering committees (ESCs) and councils whose primary purpose is threefold: (a) to communicate requirements and set priorities; (b) to develop strategies and plans; and (c) to manage execution and report on the progress of critical DHS programs. For example, S&T is a critical participant in the DHS Joint Requirements Council (JRC). The JRC is a jointly staffed departmental body tasked with managing portfolio teams chartered to advance the unity of effort goals and objectives set forth by the Secretary of Homeland Security. The portfolio teams focus on critical missions such as cybersecurity; information sharing; chemical, biological, radiological, and nuclear surveillance; aviation security; and information-based screening. S&T's role is to support select portfolio teams with identifying, coordinating, and assessing departmental capabilities, as well as to recommend courses of actions to address gaps. As a result of groups like the JRC, S&T's understanding of operational requirements and capability gaps increases and the directorate is able to propose and implement force multiplying solutions across DHS.

Direct Engagement with Operators – There is no substitution for direct engagement with operators on the frontline of homeland security. Facilitating opportunities for the directorate's scientists, engineers, and program managers to work alongside and communicate directly with the HSE is critical to the success of all projects. The trust built through these relationships and operational insight gained is why S&T continues to invest resources into these activities. Throughout these engagements, S&T employs a systems development life-cycle approach to identify and characterize the operational challenges; design a future state for operations and processes; and conduct test and evaluation activities. Two examples of ways S&T engages with operators are: (a) the Partnering for Innovation and Operational Needs through Embedding for Effective Relationships (PIONEER) program and (b) the First Responder Resource Group (FRRG). PIONEER is comprised of three programs designed to increase the number and depth of relationships between S&T and DHS components. Through participation in

THE STRATEGIC FRAMEWORK CONTINUED

PIONEER's Special Advisor, Exchange Officer, and Embed programs, S&T program managers will experience firsthand a component's operational context and increase their network of operational users. At the same time, the components will gain valuable insight into the directorate's priorities, state-of-the-art technologies, and innovative research. While the PIONEER program focuses on DHS components, the FRRG targets the first responder community. Comprised of active duty and retired first responders, the FRRG is an all-volunteer working group that helps S&T identify the top-priority needs of responders in the field. The group, whose members are drawn from a broad range of disciplines, sectors, and regions of the country, also support the solution development process.

Make Strategic Investments in High-impact, Priority Areas

The directorate's ability to make strategic investments in high-impact, priority areas is dependent upon three prerequisites: (a) the successful execution of activities designed to identify and prioritize requirements, as described in the previous section; (b) the cultivation of a balanced R&D portfolio; and (c) the continued investment in national and directorate capabilities that enable R&D. The latter two prerequisites are described in more detail in the following sections.

Balanced R&D Portfolio

Apex Programs - The strategic focus of S&T's Apex programs is directly linked to our Visionary Goals. Given the complexity and range of issues involved, these high-profile and multidisciplinary programs span three to five years and undergo quarterly reviews by an ESC. Each Apex program consists of a balanced portfolio of projects with scientifically feasible risk that span basic research to advanced technology development. Deliverables range from game-changing technical capabilities to cost-saving business processes. In fiscal year (FY) 2015, S&T dedicated roughly one-quarter of its discretionary R&D budget to eight Apex programs—Air Entry and Exit Reengineering, Border Enforcement Analytics, Border Situational Awareness, Cybersecurity in Critical Infrastructure, Relational Adaptive Processing of Information and Display, Next Generation First Responder, Real-Time Biological Threat Awareness, and Screening at Speed. Through these programs, S&T will tackle the nation's toughest security challenges—both today and in the future—with strategic and innovative solutions.

Technology Engines - A new S&T concept, the Technology Engines are centralized functions that will provide the same suite of services to all Apex programs and to S&T at large; however, they will tailor their work based on a program's individual focus and capability needs. Drawing on the expertise of S&T staff and external scientific, technical, industrial, and academic communities, the Technology Engines will proactively monitor emerging capabilities and state-of-the-art techniques in specific capability areas such as communication and networking tools, data analysis, human systems, and situational awareness. Based on this information, the Technology Engines will provide the Apex programs with best practices, reusable products and solutions, lessons learned, and technical services. The Apex programs will rely on the Technology Engines to produce high-quality solutions that keep pace with advances in the market, ensuring that investments are wisely made.

THE STRATEGIC FRAMEWORK CONTINUED

Innovation and Acquisition – Innovation and acquisition projects are designed to fulfill one of two purposes: (a) to discover breakthrough and disruptive technology that can transition within one to three years or (b) to inform and enable future end-user acquisition programs. In doing so, the innovation and acquisition projects maximize S&T's effectiveness through the research and development of force multiplying solutions. This portfolio involves applied research and advanced technology development.

Quick Reaction – Periodically, S&T receives urgent need statements from end users or inquiries from leadership regarding emerging threats and natural hazards. In these situations, S&T launches quick reaction projects to address these high-priority needs. Working with subject matter experts and leveraging off-the-shelf technologies, S&T aims to deliver capabilities and knowledge products to operators within 12 months.

Capabilities that Enable Research and Development

Capability and Solution Enablers (CaSEs) – For a technology project to be successful, leaders and developers must look beyond traditional R&D activities. Areas such as technology foraging, operational experimentation, technology transfer, commercialization, partnership management, systems analysis, test and evaluation, standards, systems engineering, and solution transition are critical to enhancing the results and outcomes of an R&D effort. Known collectively as CaSEs, S&T provides these enablers to ensure our R&D solutions are better utilized, transition more easily, and can integrate with existing solutions.

Enduring National Capabilities – S&T manages five national laboratories that develop or enhance science, technology, and engineering capabilities. While each has a specific focus—chemical security, biodefense, urban security, animal diseases, and transportation security—the labs work to ensure efforts are coordinated, are not duplicative, and support investments in high-impact, priority areas.

Chemical Security Analysis Center

National Urban Security Technology Laboratory

National Biodefense Analysis and Countermeasures Center

Plum Island Animal Disease Center

Transportation Security Laboratory

THE STRATEGIC FRAMEWORK CONTINUED

Partner with the Homeland Security Enterprise

S&T must continuously invest in the creation and maintenance of partnerships with DHS components and other R&D organizations. Internal and external partnerships are a core element of our strategy and serve as the foundation of S&T's innovative ecosystem. Whether through international agreements with allied foreign nations, grants to academic institutions, or Cooperative Research and Development Agreements with industry, S&T continually pursues new opportunities and instruments to formalize relationships with innovative organizations. Benefits from these partnerships are numerous and include diversifying investments across a broader range of operational needs, increasing technology transition, reducing programmatic risk, and leveraging other agency investments. In turn, these benefits position S&T to have the financial and analytical resources to deliver force multiplying solutions. The following activities highlight the execution of this initiative:

Innovation Centers – The Innovation Centers aim to transition capabilities to end users through cutting-edge R&D projects. Owned and operated by the DHS components, the centers will be jointly funded and staffed by S&T to provide R&D support. The Innovation Centers perform three critical functions that complement S&T's mission space and strategy: (a) coordinate internally funded component research with related S&T and DHS projects; (b) enable and/or execute technology transition activities such as late-stage technology development, rapid prototyping, and test and evaluation; and (c) foster an innovative and entrepreneurial culture that inspires new ideas, promotes stakeholder engagement and transparency, and cultivates an enduring ecosystem focused on solving critical homeland security challenges.

In-Q-Tel (IQT) – IQT serves as a bridge between federal agencies and start-up firms on the leading edge of technological innovation. In 2011, S&T formalized a strategic partnership with IQT. Pooling resources from nine federal agencies, IQT identifies, adapts, and delivers innovative technologies that solve some of the department's highest priority operational needs at a fraction of the cost. In fact, for every $1 invested by S&T we have leveraged $2.66 from other U.S. government agencies; as a result, S&T has been able to partner with the HSE for an even greater impact and return on investment.

Federal Partners – S&T partners with other federal R&D organizations to develop innovative and game-changing solutions to advance the homeland security mission. As part of this effort, S&T maintains strong partnerships with national laboratories, such as those of the Department of Energy and Department of Defense, and reaches out to other partners in areas such as agriculture, environment, health, and transportation.

Academia – S&T partners with the nation's colleges, universities, and leading academic researchers to develop customer-driven, innovative tools and technologies that solve real-world challenges, as well as to train the next generation of homeland security professionals. As part of these efforts, S&T funds 10 Centers of Excellence (COEs) that address specific homeland security challenges. For example, the newest COE—the Critical Infrastructure Resilience Center—will conduct research to understand how businesses determine acceptable risks; develop scalable, cross-sector solutions that meet national needs; pilot solutions in the real world; and prepare business cases for investing in resilient critical infrastructures and systems.

THE STRATEGIC FRAMEWORK CONTINUED

ENERGIZE THE HOMELAND SECURITY INDUSTRIAL BASE

Unlike many other industries with well-defined sets of products, technologies, and customers, the HSIB is a highly fragmented federation of product and service providers serving a broad constituency. Customers and their needs vary widely, from ships for the U.S. Coast Guard to protective gear for first responders to cyber defense tools for power plants. This degree of fragmentation means that many companies with leading-edge technologies are often small and more challenging to locate and engage. Simultaneously, federal, state, and local agencies are spending less on R&D for next-generation technologies. Therefore, it is critical that S&T collaborate with the HSIB to capitalize on industry investments in R&D and encourage the development of force multiplying solutions that defend, defeat, and mitigate threats to the nation.

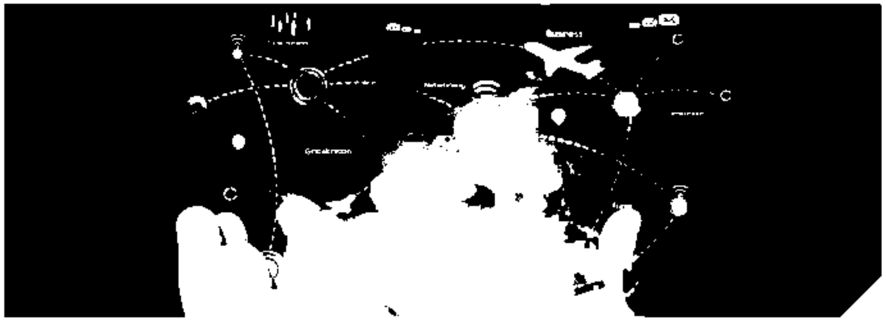
In order to energize the HSIB, S&T will revamp existing programs so industry can more easily partner with S&T. We will also develop new approaches to engage non-traditional companies. The following initiatives highlight specific activities that will help us achieve this objective.

Optimize Markets by Pooling Demand and Developing Standards

Our partners around the globe share a common mission—to ensure the safety and security of the people they serve. Most countries collaborate at an international level but largely address their challenges independently; as a result, they have limited funding to handle complex challenges and often create duplicative efforts or struggle to gain traction in a fragmented global market. S&T is working to integrate markets with international partners to draw down industry risks and incentivize product development. S&T is also working with the HSIB to consolidate R&D investments, pool demand, and accelerate the development of standards. This will improve the interoperability of technology and allow the HSIB to better plan and reduce costs. The following activities highlight the execution of this initiative:

International Engagement – S&T is in the process of creating the International Forum to Advance First Responder Technology. The forum will serve as an international platform to discuss responder challenges and issues. Responders will be able to partner on R&D initiatives through the forum and, when possible, align procurements to drive industry investments in innovative technologies and manufacturing capabilities. The forum will give responders a global voice and use common challenges and standards to create or broaden global markets for first responder technologies. Ultimately, this lowers risk for industry and incentivizes investment in more robust capabilities and product lines.

Standards Development – S&T plays a leading role in accelerating the development of standards for use by the HSE. Standards are vital in establishing best practices, achieving interoperability, supporting acquisitions, and defining grant guidance. In an effort to achieve earlier adoption of standards and inclusion in commercial products, S&T will engage industry throughout the standards development process. This approach will ensure that technologies from different manufacturers can interoperate through the use of open-source, non-proprietary solutions and standards-based approaches. Today, S&T is working on both information technology standards and physical standards.



THE STRATEGIC FRAMEWORK CONTINUED

Engage the HSIB through a Deliberate, Continuous, and Transparent Approach

S&T brings together interested parties—including responders, operational users, citizens, and academia—to engage the HSIB. Working together, each community plays a critical role in shaping the future of homeland security technology. S&T is launching new outreach mechanisms, such as online forums, to foster understanding of the homeland security market and build progress toward outcomes that will keep us all safer and minimize disruption to the pace of daily life. Additionally, S&T will use new funding vehicles like prize competitions to attract innovators who have not historically partnered with the federal government. The following activities highlight the execution of this initiative:

National Conversation on Homeland Security Technology – S&T is initiating idea exchange between operational users within the HSE and industry-based technologists. Using an online, open platform and in-person discussions, S&T is enabling end users to connect directly with technology developers. The goal of these discussions is to help industry better understand the homeland security market and create innovative and sustainable homeland security solutions.

HSIB Research and Development Coordination – S&T is exploring ways to better coordinate R&D across the HSIB, including with large commercial manufacturers and small businesses with niche capabilities. Improving coordination with this diverse community of industry partners will provide S&T insights into emerging technologies and how they can fill capability gaps. Further, S&T will work with private sector partners on rapid prototyping and identify lessons learned to better foster innovation.

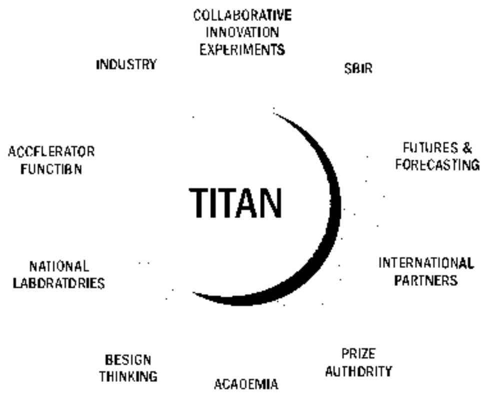
Outreach Mechanisms Designed to Engage Non-traditional R&D Performers – The landscape of technology R&D is changing as federal agencies and large corporations are no longer the dominant driver of innovation. Increasingly, advances are being discovered, developed, and distributed by non-traditional performers across every technology space. However, many of these non-traditional performers do not consider federal agencies as a potential customer market or source of funding because of the resource-intensive nature of doing business with the government. To ensure that the HSE remains on the cutting edge of technology capability, S&T must employ new methods to engage these non-traditional performers. In this regard, S&T leverages key partnerships with trade associations, innovation and start-up foundations, accelerators, incubators, the venture capital community, and entrepreneur groups to engage non-traditional partners. In partnership with these key hubs, S&T will lead interactive workshops with new communities to discuss homeland security needs that may drive technology development. S&T will also encourage new ideas from industry by launching prize competitions. Teams of companies, students, and hobbyists will be able to compete to provide viable and marketable solutions for prize funding. Additionally, S&T will host hackathons where technology developers come together to tackle a homeland security challenge in a rapid, iterative, and collaborative way. We also aim to become a leader in the broader technology scene by hosting innovation talks on scientific, cultural, and academic topics. An example of such innovative series of talks are *TED Talks™* run by the Sapling Foundation and *Virgin Disruptor* discussions run by the Virgin Group. The goal with each of these efforts is to bring new energy, resourcefulness, and ideas to the homeland security landscape.

THE STRATEGIC FRAMEWORK CONTINUED

Improve Programs Designed to Increase Collaboration with Innovative Companies

S&T and the HSIB exist in an environment of rapidly evolving threats and opportunities, and the accelerating pace of risk and technological development loom over every mission in the department. U.S. government funding remains a strong influence on basic research, but private sector investment focused on late-stage development surpassed the government's total annual R&D investments in the 1980s and has continued since then. In homeland security, innovation cycles in areas like advanced analytics, communications, additive manufacturing, and cybersecurity occur so quickly that traditional government vehicles for investment and acquisition struggle to keep up with advances and changes in technology. In order to leverage these accelerated advancements, S&T will revamp existing programs so industry can more easily partner. S&T is seeking ways to engage the investor community with an accelerator component. This program will provide S&T with insight into a range of innovation companies that can provide near- and long-term capabilities. S&T will reengineer our technology foraging approach and add a forecasting component to capitalize on industry investment trends and influence emerging technology. S&T will establish close working relationships with innovators to reduce development risk and facilitate early evaluations of solutions by operational users. S&T will also provide a flexible environment for validating and guiding the development of game-changing products and services as they approach market readiness. The following activities highlight the execution of this initiative:

Targeted Innovative Technology Acceleration Network (TITAN) – Using an arsenal of engagement tools, TITAN seeks to discover and engage innovators who are creating technologies that will enable homeland security operators to carry out their missions in new, unprecedented ways. TITAN will unify and coordinate formerly disparate activities within S&T into a cohesive program for engaging the HSIB. TITAN removes barriers that impede industry partners from working with S&T. TITAN also seeks pathways for S&T to work with industry and small businesses in a more synchronized, strategic fashion to improve the pace and quality of solution development.



TARGETED INNOVATIVE TECHNOLOGY ACCELERATION NETWORK

Responder Technology Alliance (RTA) – Through unique, strategic partnerships with first responders, the industry and investment community, and R&D organizations, RTA is tackling the most difficult and complex responder challenges. RTA will take a systems-based life-cycle approach to first responder technologies, integrating industrial design, systems engineering, cost and supply chain analysis, and market assessment. RTA is developing short-, mid-, and long-term scalable solutions that can be integrated into responder operations to strengthen

THE STRATEGIC FRAMEWORK CONTINUED

responders' health, safety, and effectiveness. Further, RTA is leading an accelerator program to create solutions at market speed. Individuals or small companies with promising solutions will be able to work directly with angel investors, venture capitalists, and responder equipment manufacturers to increase their odds of commercial success.

ESTABLISH A STRONG AND HEALTHY LEADERSHIP CULTURE

S&T's ability to achieve the aforementioned strategic objectives depends upon a common identity, clarity of mission, and leadership at all levels of the organization. With empowerment, responsibility, and accountability as cultural values, S&T strives both to create an innovation-friendly environment and to give staff the tools and development opportunities to grow and succeed within it. S&T's work environment will be educational and entrepreneurial. The workforce will be agile, inquisitive, and eager to find and execute new ideas, take informed risks, and engage external partners. To instill this culture, S&T will focus on three initiatives: (a) empower the workforce; (b) provide meaningful leadership development and professional growth opportunities; and (c) engineer a pipeline for the next generation of homeland security professionals.

Empower the Workforce

Empowering the workforce means giving a stronger voice to S&T staff and fostering a broader sense of ownership and attachment to the organization. S&T values our workforce's perspective and believes that none of us individually is as smart as all of us collectively. Moving forward, leadership will continue to integrate staff input into initiatives that affect the immediate and long-term course of the organization, such as the National Conversation on Homeland Security Technology. The following activities are intended as platforms for S&T employees to influence the organization's direction:

Employee Council – S&T will charter its inaugural Employee Council to act as a voice for S&T's workforce. Comprised of federal non-supervisory representatives, the council will identify and communicate employee perceptions on S&T programs and policies and discuss issues faced by the S&T workforce. Through the council, S&T staff will advise senior leadership on these issues and make recommendations on potential solutions. The council's recommendations and communication with senior leadership will be transparent and available to the entire workforce. The council will foster more open and clear communication between leadership and staff and ultimately make S&T's workforce more invested in the organization.

Broadening S&T Decision Making – In addition to giving staff a greater say over S&T's programs, the Under Secretary has made it a priority to decentralize decision making and delegate certain authorities to managerial levels throughout the organization. This will have the dual effect of minimizing bottlenecks for decisions that can be made at lower levels and expanding ownership of S&T's strategic direction. Examples of supporting efforts include the Apex ESC and the Project Prioritization process. The Apex ESC oversees the planning and execution of the Apex programs and Technology Engines. Chaired by each of S&T's group leads, the ESC reviews, approves, and provides resources for the Apex programs and

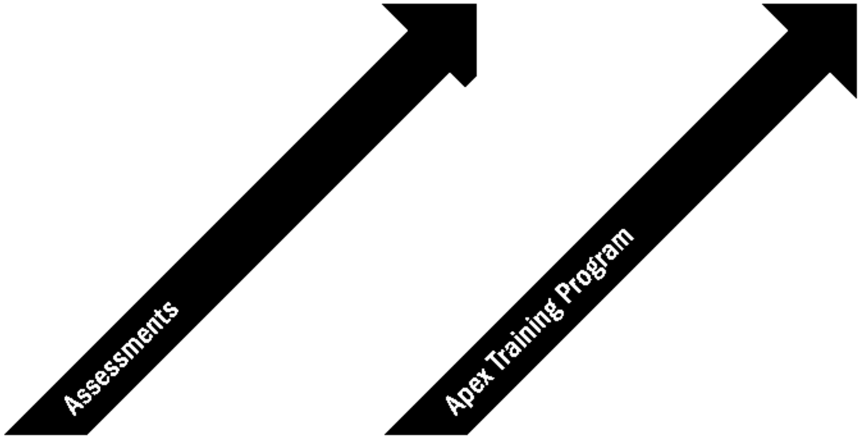
THE STRATEGIC FRAMEWORK CONTINUED

serves as the primary liaison between Apex efforts, S&T staff, and the Under Secretary. In the Project Prioritization process, representatives from across the directorate review and prioritize S&T's research, development, and innovation investments—first independently and then collectively—before presenting their recommendations to S&T leadership for approval.

Provide Meaningful Leadership Development and Professional Growth Opportunities

To arm our workforce with the skills, competencies, and knowledge to advance S&T's mission, the directorate must invest in tools, capabilities, training, and workforce development opportunities. Our robust program, which includes relevant courses at universities and colleges, encourages employees to enhance their R&D, leadership, and management skills. Specific activities to support this initiative include the following:

Assessments – S&T offers a broad range of assessments to help staff members better understand how they think and behave and how that affects them in the context of their work environment. These include 360-degree reviews and numerous popular private-sector offerings that not only improve self-awareness but also give managers tools to increase team productivity and cohesion.



Internal Opportunities Network – S&T has created a Web-based portal to advertise short-term developmental assignments within S&T and DHS to enhance employees' careers. Exposing our workforce to new experiences within the directorate and the department helps our staff develop new abilities, expertise, and relationships outside their home office.

Leadership Development – S&T offers several opportunities for leadership development, including a coaching program and leadership cohort. These opportunities emphasize personal accountability and teach participants how to model leadership through one's actions and how to create a vision.

Apex Training Program – S&T developed a unique training program for Apex program managers and team members to learn best practices and lessons learned from the original four Apex programs. Following the training program, participants understand how to use all of the organization's tools to support the execution of an Apex program.

THE STRATEGIC FRAMEWORK CONTINUED

Engineer a Pipeline for the Next Generation of Homeland Security Professionals

To ensure that the directorate continues to build on successes and evolve to meet new challenges, S&T is committed to growing a pipeline for S&T's next generation of staff. Part of this effort includes continuously assessing the organization and performing a forward-looking analysis of where staff needs will grow or decline. Based on this data, S&T will determine what expertise is needed to support S&T's mission and make long-term investments in those areas to ensure that appropriate hires are prepared to join S&T. The following two activities describes S&T's efforts to plan and develop its future workforce:

Strategic Workforce Planning – S&T will develop an enduring institutional capability to ensure projects and teams are properly resourced. This planning effort will continuously assess S&T's workforce requirements, taking into account S&T's complex mission, unique staff requirements, and the operational demands of today as well as the forecasted needs of tomorrow. S&T will also assess internal workforce-related business processes and use of hiring authorities in order to eliminate unnecessary delays while still ensuring compliance with appropriate rules and regulations.

Sourcing Talent More Effectively – As S&T begins to plan and shape its workforce more effectively, we will begin adding or connecting to talent that fills described gaps or enriches efforts already underway. This initiative will require S&T to more effectively and efficiently interface with non-government sources of expertise, build on existing relationships (e.g., use of American Association for the Advancement of Science fellowships), and take advantage of DHS's full range of career and term-limited hiring authorities. As S&T becomes more transparent and public-facing, for example through our updated website and more informative Internet presence, we will also expand our ability to connect to outside expertise.

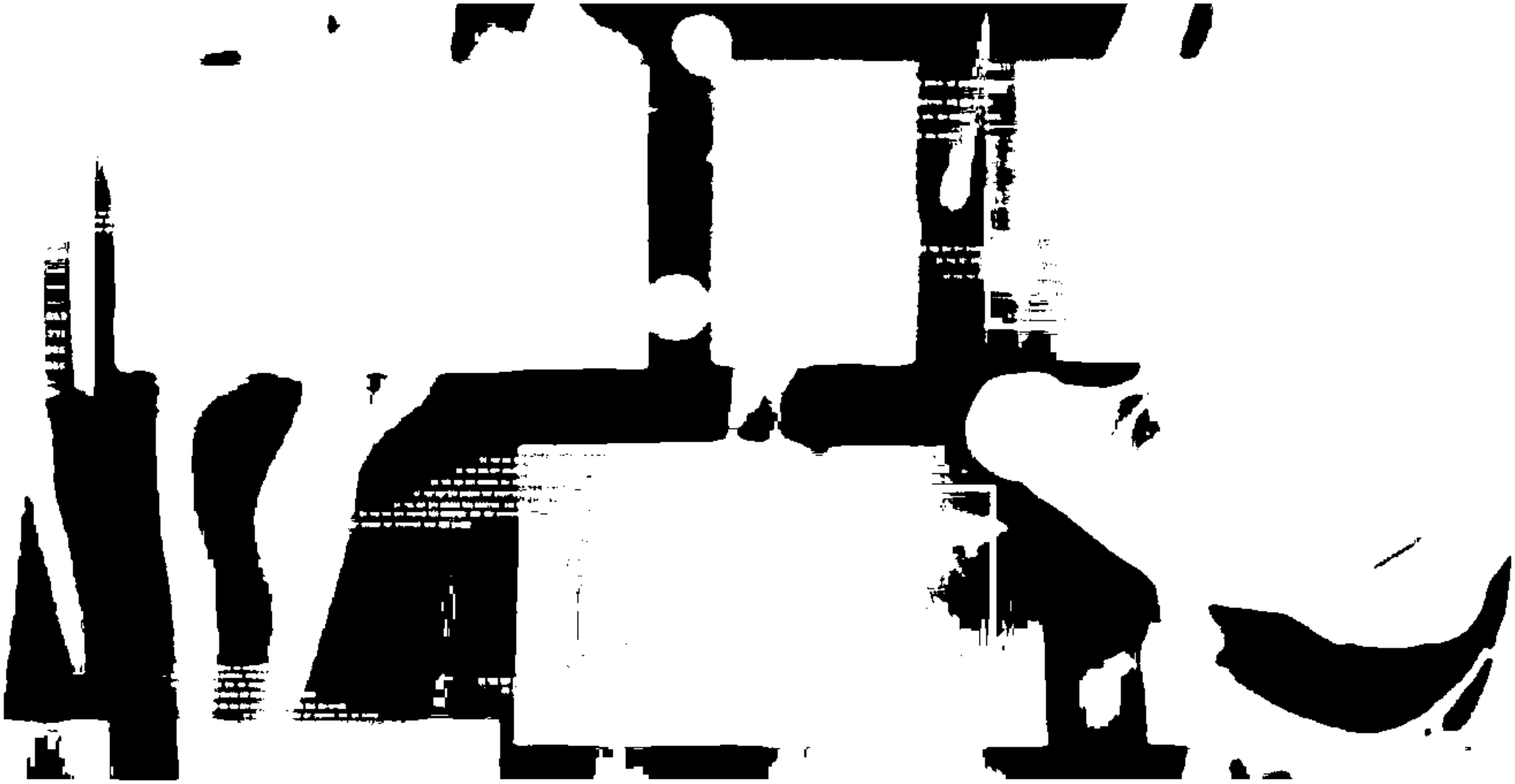
Shaping S&T's Next Generation – Faced with rapidly accelerating technologies and increasingly complex homeland security threats and challenges, S&T must prepare a future workforce that is capable of delivering specific competencies as new needs emerge. S&T will leverage its significant investment in universities to ensure a pipeline of young new employees. S&T's 10 COEs, along with our Minority Serving Institution grants and awards programs, will engage thousands of students directly in homeland security-specific coursework, scholarships, fellowships, and research opportunities. S&T will also continue to use career development grants, summer internships, and summer research teams to develop needed staff and skill sets for the future.

IMPLEMENTATION PLAN

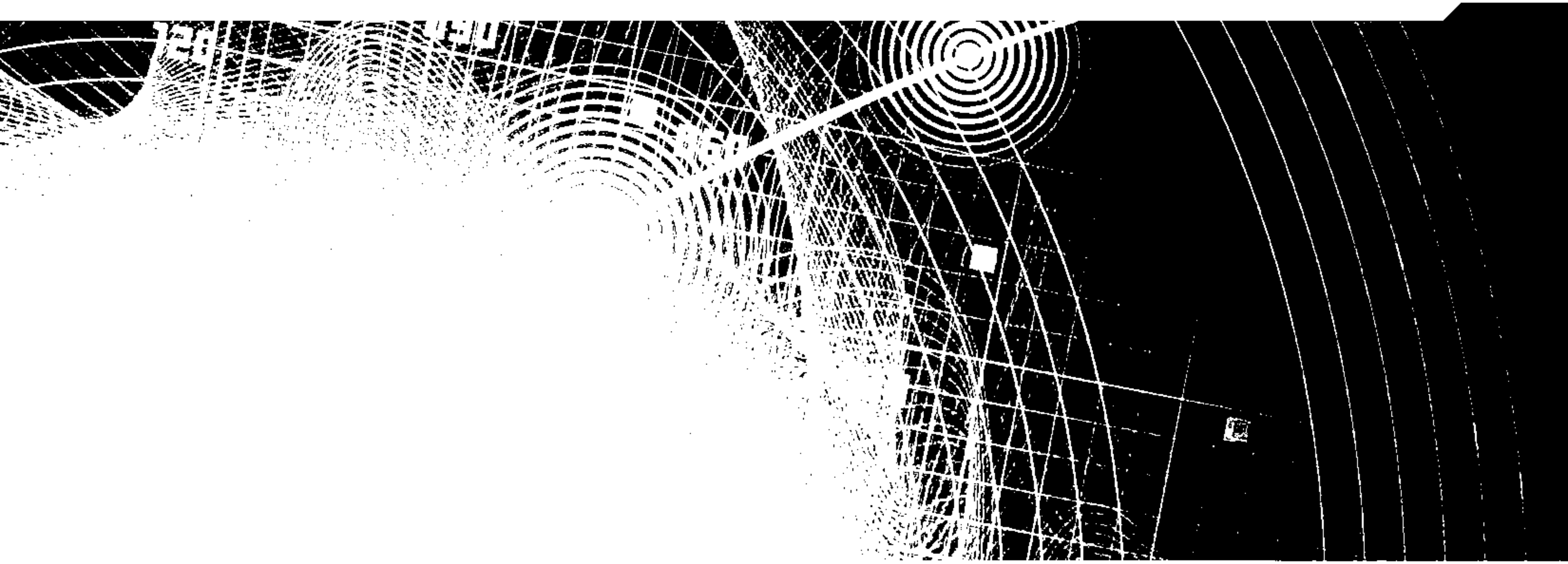
S&T STRATEGIC FRAMEWORK			Intensity of Activity (FY 2015 FY 2019)				
			FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Deliver Force Multiplying Solutions	I	Identify and Prioritize Operational Requirements and Capability Gaps	□	■	■	■	□
	II	Make Strategic Investments in High-impact, Priority Areas	■	■	■	■	■
	III	Partner with the Homeland Security Enterprise	□	■	■	■	□
Energize the Homeland Security Industrial Base	I	Optimize Markets by Pooling Demand and Developing Standards	■	■	□	□	□
	II	Engage the HSIB through a Deliberate, Continuous, and Transparent Approach	□	■	■	■	■
	III	Improve Programs Designed to Increase Collaboration with Innovative Companies	■	■	■	□	□
Establish a Strong and Healthy Leadership Culture	I	Empower the Workforce	■	■	■	■	■
	II	Provide Meaningful Leadership Development and Professional Growth Opportunities	□	■	■	□	□
	III	Engineer a Pipeline for the Next Generation of Homeland Security Professionals	■	■	□	□	□

Color Legend	Intensity Levels
Surge Effort	■
Steady-state Effort	□

S&T's implementation plan is phased over the next five years with specific levels of effort committed to the objectives, initiatives, and activities outlined in this strategic plan. Efforts committed in the first few years are designed to finish planning, including key actions and success measures, and jump-start activities designed to enable future related efforts. S&T is committed to remaining on track with the implementation plan. Quarterly reports will be provided to S&T leadership in order to assess the directorate's progress against key actions. Using this information, S&T leadership will reexamine the strategic plan on an annual basis and make any required course corrections.



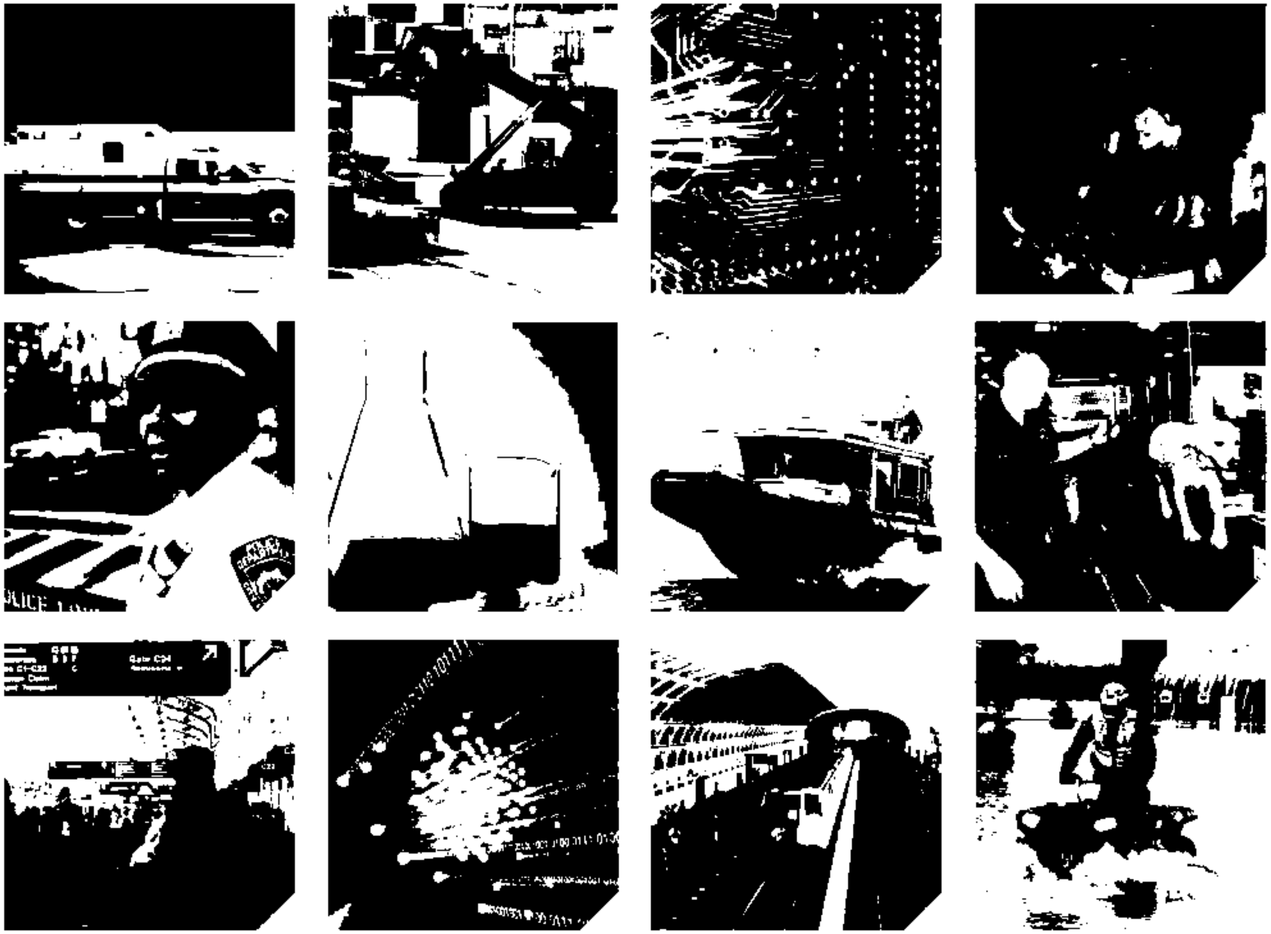
RESEARCH & DEVELOPMENT STRATEGIC PRIORITIES



Part III

RESEARCH & DEVELOPMENT STRATEGIC PRIORITIES

S&T sets R&D priorities through participation in governance bodies and discussions with mission owners. Once an investment decision has been made, S&T engages the whole of government and HSIB in order to develop a Capability Roadmap. Each of the five S&T Homeland Security Advanced Research Projects Agency (HSARPA) divisions, the three First Responders Group divisions, and Apex programs and Technology Engines have developed Capability Roadmaps aligned to the needs of their operational end users. These high-level roadmaps formalize a vision, identify strategic drivers, and list R&D objectives for the next five years. The roadmaps are constantly evolving documents and serve three primary organizational functions: (a) to build consensus among a diverse set of end users with similar operational requirements; (b) to develop a framework that directly links a strategy to tactics; and (c) to provide a framework to coordinate planning, research, development, and acquisition activities across the various groups involved.



HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS

Borders and Maritime Division (BMD)

Vision – Our long-term vision is to create a single Border and Coastal Information System (BACIS) that provides a border security information sharing environment. The BACIS will allow users to share data and tools across the entire DHS and will encompass all borders and transportation modes, including the northern and southern land borders, the coastal/maritime border, cargo and vehicles at the Ports of Entry (POEs), and people at the POEs.

Strategic Drivers - BMD's future efforts will be guided by 2014 Quadrennial Homeland Security Review (QHSR) Mission 2: Secure and Manage our Borders (specifically goals 2.1, 2.2, and 2.3), 2014 QHSR Mission 3: Enforce and Administer our Immigration Laws (specifically goal 3.2), and S&T's Visionary Goals of "Screening at Speed: Security that Matches the Pace of Life" and "Enable the Decision Maker: Actionable Information at the Speed of Thought." BMD's efforts will also be influenced by the 2014 QHSR's strategic aim to Mature and Strengthen Homeland Security by focusing on (1) integrating intelligence, information sharing, and operations; (2) enhancing partnerships and outreach; and (3) by conducting Homeland Security Research and Development. In addition, the execution of BMD's research will focus on (1) operations, innovation, and partnerships, specifically by transitioning mature and rapidly deployable solutions to DHS operational components; (2) developing technologies that have a positive impact on operations and return on investment for our customers; (3) collaborating with DHS components, other government agencies, and international partners to reduce R&D costs and time to delivery; and (4) partnering with industry to transition new technologies and guide their investments.

Description of Capabilities:

- **Land Border Security** – Develop and transition technical capabilities that strengthen U.S. land border security by safeguarding lawful trade and travel and helping to prevent illegal goods and people from crossing the border.
- **Maritime Border Security** – Develop and transition technical capabilities that enhance U.S. maritime border security by safeguarding lawful trade and travel and preventing illegal use of the maritime environment to transport illicit goods and people.
- **POE Security** – Develop and transition technologies to ensure the integrity of people and cargo that enter the United States through the POEs, including seaports, airports, and land border crossings. Enhance the end-to-end security of the supply chain, from the manufacturer of goods to final delivery, while ensuring economic throughput for the U.S. economy.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Land Border Security				
Perform operational assessments of small unmanned aerial systems (SUAS) for improved detection, identification, and classification of illicit activity and improved situational awareness in land operational scenarios. Publish reports. Transition the Slash CameraPole (one-pole configuration) to U.S. Customs and Border Protection (CBP). Install a three-pole configuration and commence operational assessments. Transition the Southwest Border Buried Tripwire to CBP. Transition a lab developmental prototype of the Tunnel Age Kit to U.S. Immigration and Customs Enforcement (ICE).	Transition the Moving Target Indicator capability to CBP. Transition the Automated Scene Understanding/Canadian U.S. Sensor Sharing Pilot capability to CBP. Transition (System 1) Unattended Ground Sensors to CBP. Field test a lab developmental prototype of the Tunnel Detection System. Field test Tunnel Age Kits.	Transition (System 2) Unattended Ground Sensors to CBP. Transition a three-pole configuration of the Slash CameraPole to CBP. Transition Low Rate Initial Production Tunnel Age Kits, a test report, and technical data to ICE.	Transition Radio Frequency Sensing Unattended Ground Sensors to CBP. Transition a prototype, test report, and technical data for the Tunnel Detection System to CBP.	Deliver a final prototype of the Tunnel Detection System and technical data to CBP's Office of Innovation and Technology Acquisition. Transition technologies to detect, locate, and disrupt border spotters employed by traffickers along the Southwest border to CBP. Transition technologies and tools to increase the safety and effectiveness of DHS operational end users.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Borders and Maritime Division (BMD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Maritime Border Security				
Install Coastal Surveillance System (CSS) operational nodes at strategic locations to improve U.S. maritime domain awareness. Perform operational assessments of SUAS for improved detection, identification, and classification of illicit activity and improved situational awareness in maritime operational scenarios. Publish reports.	Transition Integrated Maritime Domain Environment to DHS as an enterprise. Perform CSS operational demonstrations. Install CSS operational nodes at additional locations to improve U.S. maritime domain awareness. Continue to perform operational assessments of SUAS in maritime operational scenarios. Publish reports.	Transition the CSS initial operating capability to the Joint Task Force, Air and Marine Operations Center, and the U.S. Coast Guard (USCG). Install CSS operational nodes at additional locations to improve U.S. maritime domain awareness.	Deliver to DHS an integration platform for agile information sharing and discovery. Deliver to CBP; USCG; and state, regional, and local partners a coastal maritime sensor fusion system that enables cooperative maritime awareness of non-emitting vessels and the sharing of time critical, mission-useful sensor information.	Integrate CSS into USCG's Watchkeeper system. Transition technology to enhance the utilization of SUAS in the maritime domain.
Objective: Ports of Entry Security				
Finalize the United States-European Union (US-EU) Maritime Cargo Security Pilot Test Plan and preliminary assessment of the efficacy of various cargo security devices for use in the US-EU. Conduct a maritime cargo security pilot. Conduct an end to end analysis that will influence electronic chain-of-custody processes, procedures, and technology implementations. Complete CBP maritime and truck demos and Phase I Federal Protective Service demos of the government Reusable Electronic Conveyance Security Device. Develop a Border Wait Time/Supply Chain Security Roadmap. Pilot border wait time technologies.	Transition to CBP and FPS a test and evaluation analysis, a cost/benefit analysis, acquisition recommendations, and a vendors list of piloted RECONS. Transition to CBP and the governments of Mexico and Canada guidelines for the use of commercial RECONS. Transition proven border wait time technologies. Deliver the Polymerase Chain Reaction collection efficiency technology to CBP. Deliver a pollen forensic technology to CBP.	Deliver the Mobile Backscatter Scanning System upgrade to CBP. Deliver the Conveyance Void Anomaly Detector to CBP. Deliver currency detection technologies to CBP. Deliver invasive species detection technologies to CBP. Deliver counterfeit goods detection technologies to CBP.	Deliver to DHS law enforcement agencies (e.g., CBP, ICE) a secure communications and database architecture to enable law enforcement officers to access and share information securely.	Deliver an enhanced pollen forensic technology to CBP. Deliver an enhanced Polymerase Chain Reaction collection efficiency technology to CBP.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Chemical and Biological Defense Division (CBD)

Vision – CBD's work will enable society to be resilient to events involving chemical and biological agents through rapid awareness of the release of agents, effective response guidance, and efficient recovery of infrastructure.

Strategic Drivers – Multiple Presidential directives and national security strategies rely on knowledge, technologies, and guidance from DHS to ensure national readiness and preparedness for chemical and biological threats. To counter the threats ahead, CBD is taking into consideration the following strategic drivers:

- An increasing array of emerging threats added to long recognized agents enhances the complexity of the threat landscape.
- Informed assessment of the risks posed by the threat landscape is required to allocate resources wisely.
- A national biosurveillance strategy places a premium on the integration of data from multiple sources, including public health and environmental sensors, to enable rapid, well informed decisions to reduce exposures and minimize contamination spread.
- Advancing detector technology must recognize cost related barriers to implementation.
- The broad set of potential causative agents of disease requires innovation in assay development to recognize more agents with fewer assays and extend to identifying agents that may presently be unknown.
- Demonstrating recovery technologies in operational environments in concert with local, state, and national response entities is essential to developing guidance that can be readily absorbed by and transitioned to those entities.

Description of Capabilities:

- **Threat Awareness** – Develop and promote risk based approaches to inform effective prevention, preparedness, and response and recovery actions to biological and chemical terrorism events.
- **Surveillance, Detection, and Diagnostics** – Promote information integration and real-time situational awareness to reduce agent spread and enable early actions to minimize consequences to people and property. Develop trusted tools for the rapid identification and confirmation of a threat to guide appropriate response actions.
- **Response and Recovery** – Develop and incorporate a range of activities that enhance the return to normalcy after a chemical or biological contamination or animal disease event, such as developing decontamination technologies and guidelines, environmental sampling and testing methodologies, requirements for key infrastructure, and broad spectrum medical countermeasures to halt the transmission of animal diseases.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Threat Awareness				
Complete material threat assessments for priority agents in concert with interagency partners. Refine the Countermeasure Assessment and Planning tool and pilot with interagency partners.	Deploy the Bio Knowledge Management System to all Fusion Centers. Deliver updated biological, chemical, and integrated risk assessment reports. Complete field tests of large-volume releases of chlorine.	Establish an independent S&T risk assessment modeling repository. Deliver a new chemical hazards knowledge management system. Deliver the 2017 Integrated Terrorism Risk Assessment.	Deliver risk mitigation studies to DHS stakeholders for resource allocation in chemical, biological, radiological, and nuclear defense. Deliver the 2018 Biological Terrorism Risk Assessment and brief stakeholders to maximize awareness and utility of the product.	Develop an understanding of new defense capabilities that may reduce the risk and influence of biodefense investments. Deliver the 2019 Integrated Terrorism Risk Assessment.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Chemical and Biological Defense Division (CBD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Surveillance, Detection, and Diagnostics				
Complete test, evaluation, and validation of rapid real-time polymerase chain reaction (PCR), antigen, detection/diagnostics assays, and hand-held first responder assays for several Tier 1 priority agents. Initiate a demonstration project in select locations to further develop biosurveillance requirements.	Demonstrate the feasibility of low cost, sustainable environmental detection architecture. Complete development of rapid detection assays for Tier 1 priority agents and rapid anti-microbial tests for priority bio agents.	Conduct a full scale biosurveillance exercise in concert with public health and response communities. Transition validated, laboratory-based real time PCR and antigen/toxin detection assays for high consequence (Tier 1) viral and bacterial agents to the Centers for Disease Control and Prevention (CDC) Laboratory Response Network (LRN) for deployment.	Demonstrate analytics of disparate data relevant to biosurveillance objectives. Transition validated, laboratory based real-time PCR and antigen/toxin detection assays for Tier 2 bacterial threat agents to the CDC LRN for deployment.	Complete transition of validated, laboratory based real-time PCR and antigen/toxin detection assays for Tier 2 bacterial viral and toxin threat agents to the CDC LRN for deployment. Conduct independent test and evaluation of a detection system for surface transportation security.
Objective: Response and Recovery				
Initiate evaluation of decontamination technologies and advanced sampling and analysis techniques to expedite the recovery of a bio contaminated subway system.	Complete a draft interim guidance document for subway recovery. Develop analytical standards for whole genome sequencing to aid forensics.	Issue final guidance on the restoration of underground transportation systems after a biological incident. Identify common viral targets to enable construction of a foot and mouth disease panvalent vaccine.	Complete the first year of an international field trial of foot and mouth disease vaccines and diagnostics.	Demonstrate in vitro efficacy of a broad spectrum of agricultural bio therapeutic candidates.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Cyber Security Division (CSD)

Vision – CSD strives to create an HSE cyber infrastructure that is secure from cradle to grave. Secure, in this context, is defined by the following set of properties: trustworthy, dependable, robust, survivable, transparent, observable, privacy-regulated, self-aware, and self-adaptable.

Strategic Drivers – The S&T Visionary Goal "A Trusted Cyber Future, Protecting Privacy, Commerce, and Community" and the 2014 QHSR goals 4.3 and 4.4 will guide CSD's research in the years to come. CSD will aim to improve the underlying infrastructure of the digital world and ensure information is protected, illegal use of information is deterred, and privacy is not compromised. Primary technological and threat drivers include:

- The continued growth of the Internet of Things, which will result in heretofore unconnected devices interacting via the Internet.
- The interconnection of multiple aspects of life (e.g., critical infrastructure, medical devices, automobiles) that depend on digital devices and information. As this continues to expand, the impacts and consequences of these connections will become increasingly difficult to predict.
- The barriers to entry for cyber criminals, "hacktivists," and cyber terrorists will decrease, expanding the pool of those who can disrupt the cyber infrastructure.

Policy directives and implementation will also continue to impact CSD's research portfolio. Recent legislation and executive orders have, for example, established requirements for a National Critical Infrastructure Security and Resilience (CISR) R&D plan (Presidential Policy Directive-21), launched a cyber-threat intelligence integration center, and called for a Federal Cybersecurity R&D plan (Cybersecurity Enhancement Act of 2014). Policy, however, will continue to lag behind technology advances, thus creating seams or gaps in the regulation and enforcement of cybersecurity norms and development of technical solutions.

Description of Capabilities:

- **Cybersecurity Research Infrastructure** – Provide the infrastructure necessary to support cyber R&D in order to match growing and adapting threats. Make special testbeds and data sets available to the cyber research community, so researchers and developers can safely test malicious code somewhere other than on the live Internet or on real data.
- **Software Assurance** – Develop innovative approaches to reduce the risk and cost of software failures. Create new tools and techniques to improve the ability of software developers to analyze software for potential vulnerabilities. Apply new test and evaluation capabilities to correct vulnerabilities and reduce the probability and frequency of exploitation.
- **Network Security** – Define and develop network and system security metrics and techniques for mapping and modeling the networks, systems, and services that comprise the Internet so as to better understand the Internet's evolving structure and vulnerabilities.
- **Mobile, Web, and Cloud Security** – Develop technologies and approaches to secure networks, systems, and their constituent devices, including mobile devices, the Web, and the cloud.
- **Identity Management and Privacy** – Develop interoperable access control technologies to provide federal, state, and local government agencies with a cost effective way to share information without compromising the privacy of individuals (i.e., personally identifiable information) or organizations.
- **Cybersecurity Education and Training** – Improve the quality and skill set of the next generation of cybersecurity professionals by exposing students to the latest defense technologies in a competitive environment. Improve the performance and skills of Cyber Security Incident Response Teams (CSIRTs).
- **Securing Critical Infrastructure** – Protect owners, operators, and users by developing and delivering technologies across industry, government, the private sector, and academia to improve the core functions of critical sector information systems and control systems.
- **Transition to Practice** – Identify innovative, federally funded research cybersecurity research that addresses existing or imminent cybersecurity gaps, fund necessary improvements identified during pilot programs and test and evaluation activities, and transition this research into the HSE through partnerships and commercialization.
- **Cybersecurity for Law Enforcement** – Develop new technologies, capabilities, and standards to assist law enforcement in conducting investigations and forensic analysis of technologies used in criminal activity. Aid organizations in mitigating the potential impact and damage posed by insider threat activity.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Cybersecurity Research Infrastructure				
Create a legal framework and infrastructure to facilitate live streaming of data sets.	Create a program structure to support the cataloging, hosting, and/or mirroring of international data sets.	Expand the educational security courses and material offered through the Defense Technology Experimental Research testbed. Expand the legal framework to support international data sharing.	Create data enclaves to support access to restricted data sets.	Expand federated capability to support non-heterogeneous resources, allowing for experiments to span from large scale clouds to nomadic mobile devices.
Objective: Software Assurance				
Develop a systematic method to map natural language security controls to Common Weakness Enumerations.	Produce tools for identifying, analyzing, and rectifying latent vulnerabilities in software.	Pilot tools used for identifying, analyzing, and rectifying latent vulnerabilities in software.	Transition tools to commercial market and integrate into existing services.	Transition tools to commercial market and integrate into existing services.
Objective: Network Security				
Develop router traffic monitors, route tracing tools, and Internet traffic visualization tools.	Develop router traffic monitors, route tracing tools, and Internet traffic visualization tools.	Develop new tools and techniques for mapping several layers of the Internet to detect and mitigate malicious behavior.	Deliver newly developed tools that meet customer needs.	Deliver newly developed tools that meet customer needs.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Cyber Security Division (CSD)

FY 2015	FY 2016	FY 2017	FY 2028	FY 2019
Objective: Mobile, Web, and Cloud Security				
Validate the origins of internet routes through the operational use of the Resource Public Key infrastructure	Pilot near-term mobile security solutions. Pilot cloud forensics and auditing tools	Begin testing and evaluation of an initial end-to-end secure cloud architecture Test experimental deployment of the Border Gateway Protocol.	Assess produced cloud forensics and auditing technology approaches and solutions	Assess the effectiveness of developed solutions to meet evolved security requirements and document gaps Operationally deploy an end-to-end secure cloud architecture.
Objective: Identity Management and Privaey				
Conduct system integration, interoperability tests, and evaluations for federal, state, local, tribal, and territorial agencies through the Identity Management testbed. Evaluate and award research areas through a Privacy Broad Agency Announcement.	Provide fine grain, secure information access and physical access.	Address current federal, state, and local identity management requirements in line with ongoing federated activities through the Identity Management testbed.	Collaborate with international entities on the global federated identity management research needs of disparate communities.	Deliver solutions for attribute based access control while reducing identity fraud and enhancing privacy.
Objective: Cybersecurity Edueation and Training				
Test S&T funded technologies in cyber gaming challenges. Transition CSIRT best practices to U.S. and international CSIRT partners.	Test S&T funded technologies in cyber gaming challenges.	Test S&T funded technologies in cyber gaming challenges.	Test S&T funded technologies in cyber gaming challenges.	Test S&T funded technologies in cyber gaming challenges.
Objective: Securing Critical Infrastructure				
Initiate Cyber Physical Systems Security research program. Establish an automotive security consortium Complete annual R&D projects with the oil and gas subsector.	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified.	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified	Identify requirements and new partners from transportation, energy, and water sectors. Complete annual R&D projects with the oil and gas subsector and other sectors, as identified.
Objective: Transition To Practice				
Transition three technologies to the commercial market each fiscal year. Pilot three to six technologies in production environments in the HSE each fiscal year. Identify six to 10 technologies that are candidates for transition each fiscal year.				
Objective: Cybersecurity for Law Enforcement				
Test and evaluate deployable cloud forensics solutions and new capabilities in partnership with law enforcement customers.	Begin detection research, utilizing both Bayesian and machine learning approaches. Complete research and transition to DHS law enforcement components signal survey and direction finding software.	Complete operational pilots of next-generation technology architecture for law enforcement.	Deliver updated forensic solutions for law enforcement to respond to technological advances made for personal electronic devices	Pilot test personal electronic device research with the law enforcement community

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Explosives Division (EXD)

Vision – EXD protects citizens and our country's infrastructure against the devastating effects of explosives by seeking innovative approaches in detection and countermeasures. EXD provides concepts, science, technologies, and systems to increase the DHS's ability to detect explosives and mitigate the effects of an explosive blast. EXD will:

- Rapidly develop and deliver knowledge, analyses, and innovative solutions to counter the threat of improvised explosive devices (IEDs) against domestic targets.
- Leverage technical expertise to assist the efforts of the Transportation Security Administration (TSA) and other DHS components to establish operational requirements and select and acquire needed technologies.
- Conduct, catalyze, and survey scientific discoveries and inventions relevant to existing and emerging explosive materials and devices.

Strategic Drivers – Frequent and devastating attacks against U.S. commercial aviation and other domestic targets began in 1988 with the bombing of Pan Am Flight 103 over Lockerbie, Scotland. Threats today include attacks not just against aviation but also against mass transit (e.g., Madrid, London), fixed infrastructure (e.g., Murrah Federal Building), and public gatherings (e.g., Times Square, Boston Marathon). EXD endeavors to counter these threats by implementing the first goal of the 2014 QHSR: to prevent terrorist attacks. On September 9, 2014, the Under Secretary for Science and Technology testified before the House Committee on Homeland Security that "noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Whether screening people, baggage or cargo, unobtrusive technologies and improved processes will enable the seamless detection of threats while respecting privacy, with minimal impact to the speed of travel and the pace of commerce." More specific strategic guidance comes from the 2013 HSAHPA/TSA R&D Test and Evaluation Strategic Plan, which states that S&T should endeavor to "accelerate the process of delivering new capabilities to the user that improve effectiveness and efficiency" and "support risk-driven operations to provide effective and efficient security."

Description of Capabilities:

- **Aviation Solutions** – Develop cost-effective systems for screening air cargo, checked baggage, carried items, and people at checkpoints that will improve detection capabilities, reduce false alarm rates, and improve the overall customer experience.
- **Intermodal Solutions and Facilities Protection** – Develop technologies capable of screening in high-throughput areas where traditional checkpoints are neither effective nor efficient. Enhance tools to improve current canine and trace detection screening methods.
- **Foundational Science** – Determine the explosives and blast phenomenology that makes applied R&D possible. This includes the study of explosive material characteristics relevant to discrimination and detection and the assessment of blast effects on aircraft and infrastructure.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Aviation Solutions				
Develop an air cargo screening capability for X-ray images. Conduct air cargo IED studies on six high priority threats. Develop a checked baggage prototype with an automated target recognition algorithm. Develop a Coded Aperture X-Ray Imaging System. Integrate with current AT systems.	Study additional air cargo IED threats as part of the air cargo threat study. Modify least risk bomb location procedures. Develop "K" and "W band" systems with auto threat detection. Develop an advanced multi view X-ray prototype. Create a Coded Aperture Micro Mass Spectrometer Explosives Trace Detection (ETD) prototype.	Improved algorithms for checked baggage. Retrofit air cargo's ETD system. Develop Dynamic Risk Screening interfaces for checkpoint systems. Extend Advanced Imaging Technology (AIT) development for "no divestiture" screening. Develop scanning technology to extend checkpoint screening to cover liquid explosives and thin sheets.	Extend AIT development to support "walk at speed" screening. Continue development of checkpoint systems to support Tier 3 explosives and reach goal of 500 bags per hour. Work with TSA to integrate AIT and checkpoint technology with TSA concept of operations.	Transition air cargo ETD. Continue AIT development with a focus on automatic threat identification. Extend checkpoint baggage systems to support TSA goal of 600 bags per hour and detection of Tier 4 explosives.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Explosives Division (EXD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Intermodal Solutions and Facilities Protection				
Evaluate Department of Defense (DOD) sponsored standoff detection systems. Evaluate a widely tunable infrared trace source prototype. Demonstrate a person-borne standoff detection technology. Perform laboratory test and evaluation of an intelligent video algorithm with a realistic data set. Conduct operational pilots of forensic video tools providing leave-behind detection and surveillance for situational assessment.	Demonstrate vehicle eye safe trace detection advanced feasibility. Evaluate additional widely tunable infrared trace source prototypes. Transition interim standoff trace detection capabilities from DOD. Develop an Under Rail Screening System prototype. Continue developing advanced video algorithms for leave behind improvised explosive detection. Demonstrate system ability to detect leave behind, replay video, associate to individual, and tag and track the individual. Deploy an intelligent video prototype.	Demonstrate and down select a vehicle eye-safe trace detection design. Develop a layered system prototype incorporating millimeter wave imaging array. Deploy an intelligent video system in an operational environment. Conduct operational test and evaluation of the Under Rail Screening System.	Test and evaluate vehicle eye safe trace detection prototypes. Demonstrate person borne standoff detection advanced feasibility.	Pilot a vehicle eye safe trace detection prototype system at federal facilities. Deploy a layered system prototype in an operational environment. Demonstrate a non-invasive Screening at Speed prototype system for standoff explosive detection in the mass transit environment.
Objective: Foundational Science				
Develop explosive safety standards. Enhance transportation security operations. Develop capabilities to characterize explosive detection signatures. Demonstrate explosive data integration.	Provide data for high-risk chemical facilities regulation. Reduce vulnerabilities by denying resources through precursor inhibition, improving detection at target locations, and enhancing data integration. Conduct a threat informed risk analysis. Develop capabilities to characterize explosive detection signatures. Deliver component decision support tools for first responders and emergency planners regarding homemade explosives incident planning and mitigation measures.	Develop a desktop FTD prototype. Establish data sharing practices with interagency and industry partners. Develop capabilities to characterize explosive detection signatures.	Develop portable FTDs with tools and methodologies. Develop explosive detection signatures image library interface for DHS partners. Develop capabilities to characterize explosive detection signatures. Develop risk based analysis and situational awareness tools for the DHS National Protection and Programs Directorate and the interagency.	Develop enhanced capabilities to characterize explosive detection signatures.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Resilient Systems Division (RSD)

Vision – RSD is charged with identifying and developing innovative and practical solutions to enhance the nation's resilience to all hazards.

Strategic Drivers RSD's strategic drivers are based on national Presidential Policy Directives (PPD 8 and PPD 21), the 2014 QHSR, Federal Emergency Management Agency (FEMA) and DHS National Protection and Programs Directorate priorities, and the operational capabilities of the user community. Based on these drivers, RSD will develop innovative solutions that are readily deployable and tailored to the needs of DHS operational components and federal, state, and local users. RSD will collaborate with DHS components and other federal and international partners to reduce costs and accelerate technology transition. Similarly, RSD will strengthen existing and build new partnerships with the HSIB to transition R&D solutions into economically viable commercial products.

RSD's R&D strongly supports three department-wide strategic goals as defined in the 2014 QHSR. In support of Mission 1: Prevent Terrorism and Enhance Security, RSD's portfolio includes R&D to help prevent terrorist attacks and reduce risk to the nation's critical infrastructure, key leadership, and events. For QHSR Mission 4: Safeguard and Secure Cyberspace, RSD's projects help strengthen critical infrastructure security and resilience; cybersecurity; and law enforcement, incident response, and reporting capabilities. Finally, RSD supports QHSR Mission 5: Strengthen National Preparedness and Resilience through R&D activities aimed at enhancing national preparedness, mitigating hazards and vulnerabilities, ensuring effective emergency response, and enabling rapid recovery following an incident.

RSD conducts enabling activities in support of mission achievement, such as building and sustaining intergovernmental and public private partnerships and facilitating outreach and information sharing to enhance community resilience and improve public awareness and preparedness. RSD also applies social and behavioral science to improve threat detection and Countering Violent Extremism (CVE) and develops innovative approaches and effective solutions to homeland security challenges.

Description of Capabilities:

- **Cyber-Physical Systems (CPS) in the Critical Infrastructure** – Transform CPS in critical infrastructure into safe, secure, and self-healing environments. Enhance the security and continuity of critical infrastructure, with special emphasis on lifeline functions and the associated interdependencies and cascading effects.
- **Disaster Response and Recovery** - Make disaster management routine, agile, and risk-informed. Increase the agility of disaster response and strengthen the capability of communities to recover rapidly from incidents and events.
- **Resilient and Risk-tolerant Communities** Change communities into resilient and risk tolerant organizations. Improve public preparedness, awareness, and community resilience through the integration and application of social and behavioral sciences.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: CPS in the Critical Infrastructure				
Create a CPS framework, architecture, and tool set. Create system models of cross-sector cascading effects.	Deploy a CPS framework for the electric grid; conduct field test and evaluation. Deploy system models for lifeline functions.	Extend CPS framework to communications and water; conduct field tests and evaluation. Identify and develop economic incentives for adopting resilience practices and/or technologies. Develop Wearables for Infrastructure Security and Resilience (WISER).	Transition and deploy a CPS framework in the energy and power sector. Pilot economic incentives for resilience in communities. Develop and refine WISER.	Transition to multiple sectors and conduct field exercises. Deploy WISER.

HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY DIVISIONS CONTINUED

Resilient Systems Division (RSD)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Disaster Response and Recovery				
Create a system of systems decision support tool to enhance flood response and recovery. Modernize the National Hurricane Program (NHP) to speed evacuation planning.	Develop community rating metrics for the National Preparedness and Response programs. Deploy risk-based modeling and simulation tools for natural hazards planning.	Develop fusion algorithms for flood management. Develop fusion algorithms and an evacuation decision tree model for FEMA regions.	Integrate data sets for the National Preparedness and Response programs and conduct operational field tests and evaluation. Integrate models and data for NHP and start transition to FEMA operations.	Conduct field testing on the Relational Adaptive Processing of Information and Display Apex program. Deploy updated NHP system within FEMA and state and local regions.
Objective: Resilient and Risk-tolerant Communities				
Establish an international community for CVE. Transition the Terrorism and Extremist Violence in the United States (TEVUS) database. Start CVE engagements with Australia, Israel, and the United Kingdom.	Develop a CVE strategy. Build a knowledge repository on CVE trends, indicators, and lessons learned. Research social and behavioral factors related to public messaging and CVE activities.	Execute further research to understand, identify, and divert violent extremism. Build community cohesion and communicate a counter narrative. Continue social and behavioral research related to public messaging and CVE activities.	Scale and expand CVE engagement with Five Eyes nations. Apply results of social and behavioral research to improve the effectiveness of public messaging and government CVE activities.	Deploy CVE products for the law enforcement community, fusion centers, and other federal agencies.

FIRST RESPONDERS GROUP DIVISIONS

First Responder Technologies (R-Tech)

Vision – First responders will have the force multiplying tools and solutions that allow them to save lives and maximize preparedness.

Strategic Drivers – A major strategic driver is consistency with department wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Additionally, R-Tech's strategic priorities are driven by the needs of first responders who want more situational awareness and protection when they approach an incident.

Description of Capabilities:

- **Personal Protective Equipment (PPE) and Tools** – Develop advanced PPE and tools for first responders to protect lives, increase their safety, and mitigate damage.
- **3-D Location and Response Awareness** – Deliver geo location integrated technologies that track first responders, threats, and resources available to support response operations.
- **Technology Clearinghouse** – Provide a first responder technology clearinghouse that enhances technical information exchanges, delivers advanced training tools, and ensures the validity of software.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: PPE and Tools				
Develop Phase II Multi-Threat Textile to provide first responders with enhanced protection from stabbing, fire, biological, and other hazards. Conduct performance testing on prototype materials and write report.	Develop a Thermal Imaging Camera that can be integrated into a self contained breathing apparatus (SCBA) to provide first responders with enhanced on scene imagery while fighting fires. Conduct an operational field assessment of the thermal imaging camera and write report.	Commercialize Finding Individuals for Disaster and Emergency Response (FINDER) tool, which provides urban search and rescue teams with the ability to detect human heartbeats in rubble or buildings during a disaster.	Develop tools to increase exposure detection of unknown threats such as toxins, biological agents, or contaminants during response operations. Conduct an operational field assessment of detection tools.	Create self-decontaminating PPE to provide protection against biological agents, by providing an effective barrier to bacteria, which is innocuous to the human wearer and is lightweight and breathable. Conduct performance testing on PPE and write report.
Objective: 3-D Location and Response Awareness				
Commercialize Improved Structure Firefighting Glove to provide on scene firefighters with enhanced dexterity and donn/doff ability.	Develop enhanced mobile biometrics, to provide on scene first responders with iris, face, and fingerprint readers to assist them in obtaining accurate near real-time identifications. Conduct an operational field assessment of mobile biometric tools.	Develop Lost Person Locator Tool for first responders to use when searching for lost individuals. Publish guidance, protocols, and strategies for the lost person locator tool.	Develop a system to detect, monitor, and analyze passive and active threats and hazards at incident scenes. Conduct an operational field assessment of above system.	Develop persistent surveillance tools to enhance a first responder's awareness of on-scene threats and hazards. Conduct an operational field assessment of persistent surveillance tools and write report.
Objective: Technology Clearinghouse				
Begin transition of the Virtual Training module, to provide first responders with realistic training scenarios that enhance their skills and confidence to respond effectively and efficiently during real-life incidents.	Finalize transition of the Virtual Training module to the first responder community.	Upgrade First Responder Support Tools (FiRST) app to include enhanced situational awareness of explosive threats.		

FIRST RESPONDERS GROUP DIVISIONS CONTINUED

Office for Interoperability and Compatibility (OIC)

Vision - First responders and the public will always have the emergency preparedness, mitigation, response, and recovery information they need.

Strategic Drivers A major strategic driver is consistency with department wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Also, OIC's strategic priorities are consistent with the One DHS Executive Committee Strategy Goal 1: Integrate and enhance emergency communications capabilities through common enterprise architecture. Additionally, OIC's strategic priorities are driven by the needs of first responders who seek interoperability and compatibility research, development, testing, and evaluation expertise that focuses on bridging land mobile radio (LMR) and broadband networks and improving LMR network efficiency.

Description of Capabilities:

- **Voice and Data Communications** Empower first responders to talk to each other and share data without worrying about underlying technology.
- **Information Sharing** - Enable first responders to securely exchange useful, actionable information in time to make a difference.
- **Alerts, Warnings, and Notifications (AWN)** Articulate a rational, integrated approach to AWN for all hazards and all threats.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Voice and Data Communications				
Develop capabilities for LMR Long Term Evolution (LTE) interoperability. Develop concepts for a First Responder Personal Area Network (PAN). Develop a business process model to establish baseline costs of Project 25 (P25) performance, conformance, and interoperability testing.	Establish a 700 MHz demo network. Transition LMR-LTE interoperability capabilities to first responders. Develop and test the initial architecture of the First Responder PAN. Support public safety broadband (FirstNet) architecture development. Establish testing capabilities to determine LMR conformance with the P25 suite of standards.	Conduct security research and testing of 700 MHz network and LMR-LTE interoperability. Integrate the First Responder PAN technology with LMR and LTE. Support FirstNet architecture development. Transition the First Responder PAN technology for operational use. Initiate a P25 conformance testing program.	Add on capabilities for LMR, including audio and video quality tools. Conduct P25 testing. Support FirstNet architecture development. Conduct P25 testing.	Release the Video Quality in Public Safety Handbook v3. Conduct P25 testing. Support FirstNet architecture development.
Objective: Information Sharing				
Standardize computer-aided dispatch (CAD) and mutual aid information sharing. Transition first responder collaboration tools.	Transition CAD and mutual aid standardization tools. Design architectural concepts for the public safety cloud (PSC), including identity and access management (IdAM) requirements.	Develop PSC standards and demo projects. Conduct IdAM application demonstrations, including a Backend Attribute Exchange Pilot. Conduct an Internet of Things demonstration.	Transition PSC technologies for operational use. Develop next generation 911 standards. Develop standards for Internet of Things use by first responders.	Develop and transition technologies to allow first responders to securely exchange information as needed.
Objective: Alerts, Warnings, and Notifications				
Conduct Wireless Emergency Alerts webinars. Develop a public AWN architecture.	Release the Emergency Data Exchange Language Common Alerting Protocol Report.	Develop geo-targeted AWN. Define the next generation 911 interface.	Develop approaches and standards for citizen to government AWN.	Demonstrate citizen-to-government AWN, including next generation 911 and other methods.

FIRST RESPONDERS GROUP DIVISIONS CONTINUED

National Urban Security Technology Laboratory (NUSTL)

Vision – First responders will have the test, evaluation, and assessment services and radiological nuclear response recovery tools they need.

Strategic Drivers – A major strategic driver is consistency with larger department wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Additionally, NUSTL's strategic priorities are driven by the needs of first responders who want to understand and inform the development of emerging technologies for the public safety community in various operational field environments.

Description of Capabilities:

- **Tests, Evaluations, and Assessments** - Ensure effectiveness, performance, and suitability of technologies for operational deployment.
- **Technical Advisors to First Responders** – Bridge the knowledge gap between technology developers and end users.
- **Radiological Nuclear Response and Recovery** – Save lives, minimize economic impact, and enhance resiliency following a radiological or nuclear event.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Tests, Evaluations, and Assessments				
Conduct NUSTL Urban Operational Experimentation.	Improve the impact of the System Assessment and Validation for Emergency Responders program.	Test first responder technologies for HSARPA divisions.	Conduct SAFETY Act validation and verification testing.	Serve as a FEMA grant acquisition and quality assurance test agent.
Objective: Technical Advisors to First Responders				
Host the New York Area Science and Technology Forum.	Provide training and exercise support to first responders.	Upgrade the Sensitive Compartmented Information Facility.	Develop standards for first responder technologies.	Develop and lead alliance of laboratories supporting first responders.
Objective: Radiological Nuclear Response and Recovery				
Establish improvised nuclear device decision making skill requirements.	Develop science based tactical response guidance for a Radiological Dispersion Device.	Research disaster resilient communications and post-event messaging.	Develop tools for decision making based on radiological data. Develop guidelines for radiological operational support specialist positions under the National Incident Management System.	Provide emergency dosimetry guidance for radiological emergencies.

APEX PROGRAMS

Apex Program – Air Entry/Exit Re-engineering (AEER)

Vision - The Apex AEER program will transform immigrations and customs inspections of international air travelers traveling through the busiest U.S. international airports. The program is a collaborative effort between CBP and a multi disciplinary team from S&T to analyze existing CBP Office of Field Operations processes and identify, develop, test, and evaluate new concepts of operations and approaches to enhance and facilitate traveler screening processes. The program will also develop recommended approaches and technologies to provide CBP with cost-effective and integrated biometric entry and exit capabilities. With these solutions, CBP will be able to increase its ability to confirm the identity of persons entering and departing the United States; fulfill its obligation to implement a biometric air exit solution mandated by Congress; and ensure that processes are efficient and continue to facilitate international travel, tourism, and economic growth.

Strategic Drivers CBP is responsible for enforcing U.S. immigration and customs laws, while also facilitating international trade and travel beneficial to our economy. Increases in international air travel are straining CBP resources, resulting in increased wait times and delays for passengers to clear Federal Inspection Service areas. Additionally, DHS is statutorily required by 8 U.S.C. 1365b(d) to provide biometric entry and exit data and by 8 U.S.C. 1187(i), which requires an exit system that matches biometric information of foreign travelers against relevant watch lists and immigration information. Furthermore, the Presidential National Travel and Tourism Strategy requires DHS to take additional steps to expedite the entry process and reduce wait times for travelers. There are three primary drivers for AEER: a) facilitate trade and travel; b) implement new and improved operational capabilities required by federal legislation; and c) support the Presidential National Travel and Tourism Strategy.

Description of Capabilities:

- **Maryland Test Facility and Scenario-based Testing** - Provides a low-cost, adaptive, and configurable controlled environment for laboratory and scenario-based testing to evaluate biometric technologies, processes, and concepts of operation under realistic, simulated airport entry and exit conditions.
- **Business Case Analysis** - Assess proposed biometric and non-biometric solutions and select those that are deemed most suitable for an operational field trial. Develop a Business Case Analysis that contains cost estimates, such as infrastructure enhancements, staffing, and technology to inform potential CBP business process transformation, system development, and technology acquisition.
- **Operational Field Trial** - Conduct a field trial at an air POE to determine the performance of a complete biometric exit system under real-world conditions.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Maryland Test Facility and Scenario-based Testing				
Complete scenario-based test and evaluation. Transition entry business transformation initiatives to CBP.	Support preparations for a field trial in an operational setting. Transition entry business transformation initiative to CBP.	(Apex AEER ends in FY 2016)		
Objective: Business Case Analysis				
Deliver biometric exit business case analysis inputs.	Deliver a Business Case Analysis to CBP for acquisition follow up and development of draft acquisition documentation.			
Objective: Operational Field Trial				
Select airport site candidates for field evaluation; select biometric technology candidates for field evaluation.	Initiate and complete field trial evaluation. Transition exit field trial system technical specifications to CBP.			

APEX PROGRAMS CONTINUED

Apex Program – Border Enforcement Analytics Program (BEAP)

Vision – BEAP combines emerging data analytics capabilities with ICE senior agent knowledge to create data-driven methodologies that directly support key goals for the Administration's Export Control Reform initiatives, counter-proliferation efforts led by ICE's Homeland Security Investigations (HSI), and the interagency Export Enforcement Coordination Center (E2C2). The program flattens access to relevant data sources and makes tools available that enable rapid access to information used in enforcement actions. Using the BEAP model for counter-proliferation investigation support, S&T is translating capabilities to additional relevant investigation domains within HSI.

Strategic Drivers – There are three primary drivers for BEAP: a) improving export controls for critical commodities and technologies; b) Presidential Executive Order 13558, which established E2C2; and c) United Nations Security Council Resolution 1540 regarding non-proliferation controls for materials related to weapons of mass destruction. ICE HSI leads E2C2 and maintains unique authorities to access data sources related to export enforcement.

Description of Capabilities:

- **Exploratory Methods Mapping (EMM)** – Record knowledge from retired ICE agents with more than 30 years of experience in order to identify methods and algorithms that can identify illicit activity in data sets.
- **S&T Enclave (STE)** - Create an exploratory laboratory where technical capabilities are mapped to agent-created methods and algorithms. Conduct performance assessments to improve the computation and accuracy of results.
- **Big Data Environment (BDE)** – Deploy development operations and operations support systems to integrate successful algorithms that are successful in the S&T environment.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Exploratory Methods Mapping				
Demonstrate new algorithms to ICE leadership and Special Agent in Charge offices. Transition three key algorithms to BDE to support HSI and E2C2 operations.	Transition EMM operations to ICE HSI and E2C2.	(Apex BEAP ends in FY 2016)		
Objective: S&T Enclave				
Complete studies of Internet Protocol geocoding and entity resolution for ICE. Transition geo-coding and entity resolution results to BDE.	Transition STE operations to the HSARPA Data Analytics Engine portfolio.			
Objective: Big Data Environment				
Complete the transition and integration of BDE to ICE HSI operations. Fully implement support for additional investigation domains.	Transition BDE operations to ICE HSI, Chief Information Officer, and E2C2.			

APEX PROGRAMS CONTINUED

Apex Program – Border Situational Awareness (BSA)

Vision - CBP and partner law enforcement agencies at the federal, state, local, tribal, and international levels need improved situational awareness to more effectively and efficiently deploy resources to the areas of highest risk, particularly along land borders or the U.S. Southwest border. The Apex BSA program will enable the HSE to increase border situational awareness, leading to increased border incursion detection, interdictions, and deterrence. The Apex BSA program will improve border situational awareness by establishing an enterprise capability to a) access more data sources; b) make available decision support tools to translate available data into actionable information and intelligence; and c) share that actionable information and intelligence with partner law enforcement agencies.

Strategic Drivers - BSA's future efforts will be guided by 2014 QHSR Mission 2: Secure and Manage our Borders (specifically goals 2.1 and 2.3), 2014 QHSR Mission 3: Enforce and Administer our Immigration Laws (specifically goal 3.2), and S&T's Visionary Goal "Enable the Decision Maker: Actionable information at the Speed of Thought." BSA's efforts will also be influenced by the 2014 QHSR's strategic aim to Mature and Strengthen Homeland Security by focusing on (1) integrating intelligence, information sharing, and operations; (2) enhancing partnerships and outreach; and (3) conducting homeland security R&D. BSA will derive much of its requirements from the DHS Campaign Plan for Securing the U.S. Southern Border and Approaches (Jan 23, 2015). In addition, the execution of BSA's research will focus on (1) operations, innovation, and partnerships, specifically by transitioning mature and rapidly deployable solutions to DHS operational components; (2) developing technologies that have a positive impact on operations and return on investment for our customers; (3) collaborating with DHS components, other government agencies, and international partners to reduce R&D, operation, and maintenance costs, as well as time to delivery; and (4) partnering with industry to transition new technologies and guide their investments.

Description of Capabilities:

- **Enterprise Information Sharing Architecture** - Build the system architecture: leverage existing Intelligence Community, DOD, and DHS investments. Ingest existing data sources currently in operational use. Integrate existing cost effective decision support tools (e.g., analysis, fusion, visualization).
- **Tactical Decision Support and Mobile Communications Solutions** - Focus on border patrol station-level tactical use cases defined through field stakeholder workshops. Integrate technologies for low bandwidth/mobile users (e.g., tactical technologies). Integrate emerging decision support tools to inform tactical level decisions.
- **Strategic Planning and Resource Decision Support Solutions** - Focus on DHS use cases defined through stakeholder workshops. Integrate risk assessment tools to inform manpower and equipment resource allocation. Integrate strategic planning and resource decision support tools as needed.

FY 2015	FY 2D16	FY 2017	FY 2D18	FY 2D19
Objective: Enterprise Information Sharing Architecture				
Initiate the program and obtain ESC approval. Perform requirements analysis of Enterprise Information Sharing Architecture capability.	Develop Enterprise Information Sharing Architecture capability.	Pilot, validate, and transition Enterprise Information Sharing Architecture capability.		
Objective: Tactical Decision Support and Mobile Communications Solutions				
		Perform requirements analysis and initiate development of Tactical Decision Support and Mobile Communications Solutions capability.	Develop, pilot, and validate Tactical Decision Support and Mobile Communications Solutions capability.	Transition Tactical Decision Support and Mobile Communications Solutions capability.
Objective: Strategic Planning and Resource Decision Support Solutions				
			Perform requirements analysis of Strategic Planning and Resource Decision Support Solutions capability.	Develop Strategic Planning and Resource Decision Support Solutions capability.

APEX PROGRAMS CONTINUED

Apex Program – Relational, Adaptive Processing of Information and Display (RAPID)

Vision – This Apex program will make communities more resilient to disruptive events through the creation and application of a decision support system-of-systems for community risk assessment and resilience planning. This program aims to save lives, reduce property losses, and enhance overall resilience. The flood hazard is the first use case.

Strategic Drivers - A major strategic driver is consistency with larger department-wide strategic frameworks, including the goals under 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Also, FEMA and partner communities (state, local, tribal, territorial) need better quality data and improved awareness to more effectively respond to and plan for flood events in support of FEMA Strategic Priority 4: Enable Disaster Reduction Naturally.

The RAPID Apex program supports implementation of Presidential Policy Directives 8 and 21–National Preparedness, and Critical Infrastructure Security and Resilience, respectively–as well as FEMA's Federal Flood Risk Management Standard and Executive Order 13690, Establishing a Federal Flood Risk Management Standard and a Process for Further Soliciting and Considering Stakeholder Input. The RAPID Apex program directly links to S&T's Visionary Goals, which were informed and validated by the stakeholder community.

Description of Capabilities:

- **Community Rating System Demonstration Study** – Identify indicators of resilience in National Flood Insurance Program communities participating in the Community Rating System (CRS).
- **Data Roadmap** – Create a data roadmap identifying critical data sources sufficient to support resilience indicators and all emergency support functions.
- **Community Performance Benchmarking** – (a) Conduct pilot studies in six CRS communities with historic flood performance data; (b) validate resilience indicators from a CRS demo study; and (c) identify any new resilience indicators.
- **Community Pilots** – Conduct three regional pilots to determine the effectiveness of the resilience indicators across scales (e.g., mutual aid).
- **Technology Portfolio** - (a) Study the impact of technology solutions on communities and generate cost/benefit metrics and (b) quantify three to five critical technology solutions for each critical infrastructure lifeline function for low-, medium-, and high-risk/cost tolerances by FEMA region.
- **Decision Support Logic** - (a) Create algorithms to support common decision support needs; (b) create backend interfaces with algorithms, data sets, and analytics; and (c) create a user interface.
- **Transition to Use** – Field test applications in three to five events and exercises in two FEMA regions. Iterate development of the user interface based on feedback.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Community Rating System Demonstration Study				
Identify indicators of resilience in communities participating in the National Flood Insurance Program's CRS.				
Objective: Data Roadmap				
Create a data roadmap identifying critical data sources sufficient to support resilience indicators and all emergency support functions.				

APEX PROGRAMS CONTINUED

Apex Program – Relational, Adaptive Processing of Information and Display (RAPID)

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Community Performance Benchmarking				
	Conduct pilot studies in six CRS communities with historic flood performance data. Validate resilience indicators from a CRS demo study. Identify any new resilience indicators.			
Objective: Community Pilots				
	Conduct three regional pilots to determine the effectiveness of the resilience indicators across scales (e.g., mutual aid).	Continue regional pilots.		
Objective: Technology Portfolio				
	Study the impact of technology solutions on communities and generate cost/benefit metrics.	Quantify three to five critical technology solutions for each critical infrastructure lifeline function for low-, medium-, and high-risk/cost tolerances by FEMA region.		
Objective: Decision Support Logic				
	Create algorithms to support common decision support needs. Create backend interfaces with algorithms, data sets, and analytics. Create a user interface.			
Objective: Transition to Use				
				Field test applications in three to five events and exercises in two FEMA regions. Iterate development of the user interface based on feedback.

APEX PROGRAMS CONTINUED

Apex Program – Next Generation Cyber Infrastructure

Vision – S&T partners with the Financial Services Sector to develop and deliver advanced sensing technologies, situational understanding, response and recovery, and network protections to the institutional, sector, and cross sector levels.

Strategic Drivers – The S&T Visionary Goal "A Trusted Cyber Future: Protecting Privacy, Commerce, and Community" and the 2014 QHSR goals 4.3 and 4.4 will guide CSD's research in the years to come. CSD will aim to improve the underlying infrastructure of the digital world and ensure information is protected, illegal use of information is deterred, and privacy is not compromised. Primary technological and threat drivers include:

- The continued growth of the Internet of Things, which will result in heretofore unconnected devices interacting via the Internet
- The interconnection of multiple aspects of life (e.g., critical infrastructure, medical devices, automobiles) that depend on digital devices and information. As this continues to expand, the impacts and consequences of these connections will become increasingly difficult to predict.
- The barriers to entry for cyber criminals, "hacktivists," and cyber terrorists will decrease, expanding the pool of those who can disrupt the cyber infrastructure.

Policy directives and implementation will also continue to impact CSD's research portfolio. Recent legislation and executive orders have, for example, established requirements for a National CISR R&D plan, launched a National Cyber Threat Intelligence Integration Center, and called for a Federal Cybersecurity R&D plan (Cybersecurity Enhancement Act of 2014). Policy, however, will continue to lag behind technology advances, thus creating seams or gaps in the regulation and enforcement of cybersecurity norms and development of technical solutions.

Description of Capabilities:

- **Advanced Sensing Technologies** – Improve measurement and attestation to reveal the presence or absence of attacker modifications to network infrastructure and model network behavior.
- **Situational Understanding** – Develop sensor correlation capabilities (alerts and human inputs) to present relevant observations of human understanding and the capability to characterize the underlying digital infrastructure from the routing to network layers.
- **Response and Recovery** – Develop the capability to execute rapid, policy based, and situation specific responses, including but not limited to reconfiguring sensor grids to clarify a situation, reconfiguring systems and networks to maintain operationally critical services, and returning a network to its last known valid and secure state.
- **Network Protection** – Advance network control planes, including but not limited to secure routing for Distributed Denial Of Service protection, secure route origination and end to end routing, secure dynamic enclaves, or demand asset control to maintain network essential services, and secure browsing.
- **Operational Exercises** – Deliver the capability and capacity to run realistic exercises from the institutional level up to sector wide.
- **Common Messaging and Interfaces** – Develop or leverage common message traffic protocols to improve information sharing, including cyber threat indicators.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Advanced Sensing Technologies				
Expand current insider threat body of knowledge and initiate improved measurement mechanisms research.	Identify, pilot, and transition one to two advanced sensing technologies.	Identify, pilot, and transition one to two advanced sensing technologies.	Identify, pilot, and transition one to two advanced sensing technologies.	Identify, pilot, and transition one to two advanced sensing technologies.
Objective: Situational Understanding				
Characterize networks based on passive traffic analysis and other attributes.	Identify, pilot, and transition one to two situational understanding technologies.	Identify, pilot, and transition one to two situational understanding technologies.	Identify, pilot, and transition one to two situational understanding technologies.	Identify, pilot, and transition one to two situational understanding technologies.
Objective: Response and Recovery				
Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.	Identify, pilot, and transition one to two response and recovery technologies.

APEX PROGRAMS CONTINUED

Apex Program – Next Generation Cyber Infrastructure

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Network Protection				
Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.	Identify, pilot, and transition one to two network protection technologies.
Objective: Operational Exercises				
Conduct one to two operational exercises.	Conduct one to two operational exercises.	Conduct one to two operational exercises.	Conduct one to two operational exercises.	Conduct one to two operational exercises.
Objective: Common Messaging and Interfaces				
Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.	Ensure, to the maximum extent possible, developed and transitioned technologies use common messaging and interface standards.

APEX PROGRAMS CONTINUED

Apex Program – Next Generation First Responder (NGFR)

Vision – The NGFR Apex program envisions a responder of the future who is protected, connected, and fully aware. Armed with comprehensive physical protection, interoperable tools, and networked threat detection and mitigation capabilities, cross functional responders of the future will be better able to serve their communities. The NGFR Apex program will integrate existing and emerging communications technologies and sensors into responders' protective garments and standard equipment, making each responder a mobile, wireless communications hub and sensor platform linked automatically to a wide-ranging mesh network.

Strategic Drivers A major strategic driver is consistency with larger department wide strategic frameworks, including the goals under the 2014 QHSR Mission 5: Strengthen National Preparedness and Resilience (i.e., enhance national preparedness, mitigate hazards and vulnerabilities, ensure effective emergency response, and enable rapid recovery). Also, the NGFR Apex program is consistent with the One DHS Executive Committee Strategy Goal 1: Integrate and enhance emergency communications capabilities through common enterprise architecture. Moreover, the NGFR Apex program is directly linked to S&T's Visionary Goals, which were informed and validated by the stakeholder community.

Description of Capabilities:

- **Real-time Situational Awareness** Develop game changing tools for wearable, interoperable communications systems; indoor tracking of first responders; and incorporation of information from multiple and nontraditional sources (e.g., crowdsourcing, social media) into incident command and operations.
- **Duty Uniforms and PPE** Provide detection, monitoring, and analysis of passive and active threats and hazards at incident scenes in real time.
- **Responder Technology Alliance** - Harness the HSIB and venture capital to enable collaborative commercialization of technologies.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Real-time Situational Awareness				
Develop baseline requirements, assess technologies, define an architecture, and build a technology roadmap.	Demonstrate wearable technology, Mobile Ad Hoc Networking, and Long Term Evolution prototype.	Provide tools for real-time tracking of incidents and units. Enhance pre-loading of data.	Develop a fully aware hands-free display that provides dynamic data and is voice-activated.	Demonstrate full two-way data sharing between first responder agencies and practitioners.
Objective: Duty Uniforms and Personal Protectiue Equipment (PPE)				
Define performance criteria and identify operational, testing, and evaluation requirements for duty uniforms and PPE.	Produce 150 "America's Missing: Broadcast Emergency Response" prototype garment ensembles for DHS.	Conduct extended operational field assessments and down-select prototypes.	Conduct wearable technology pilots.	Conduct wearable technology pilots.
Objective: Responder Technology Alliance				
Develop Responder of the Future: Industrial Visionary Design.	Develop systems engineered solution management plans and launch responder technology accelerators.	Develop responder of the future enterprise technologies to link responders and operation centers.	Achieve commercialization and supply chain acceptance of responder technology through responders, industry, the investment community, and R&D organizations.	Achieve commercialization and supply chain acceptance of responder technology through responders, industry, the investment community, and R&D organizations.

APEX PROGRAMS CONTINUED

Apex Program – Real-time Biothreat Awareness

Vision – The Real-time Biothreat Awareness Apex program aims to minimize the consequences from the release of chemical and biological agents. The program will reduce the time it takes for decision makers to take action. This will be accomplished through improved situational awareness of a bio-event, consistent messaging across federal, state, and local stakeholders resulting in effective response guidance, and efficient recovery of infrastructure to normal use.

Strategic Drivers - CBD's Apex core requirements draw from multiple national policy documents including, National Biosurveillance Science and Technology Roadmap (2013), National Strategy for BioSurveillance (2012), 2014 QHSR, and National Biosurveillance Integrated Center Strategic Plan on Biosurveillance (2012).

The primary technology and threat drivers include:

- Threat agents are more accessible than ever, and the proliferation of technology has made it easier for non-state actors to enhance existing pathogens, or engineer new pathogens allowing them to remain undetected by traditional detection methods.
- Readiness and preparedness requires early identification of significant health incidents involving naturally occurring, accidental, or man-made threats to inform and alert decision makers.
- Well-informed decisions require the integration of contextual information derived from multiple data sources from public health networks and environmental sensors in nearly real time.
- Current capabilities in the U.S. government do not aggregate data and inform decision makers in a timely manner.

Description of Capabilities:

- **Requirements** – Determine the information needed to affect a response, develop environmental sensors that detect bio-threats at levels relevant for public health that differentiate near neighbor bio-agents, demonstrate technology triggers that inform short-term actions that include rapid confirmatory testing, evaluate bio-threat detection capability orthogonal to PCR, identify the contextual data needed to inform decision makers in order to appropriately address the desired response.
- **Integration** – Implement interconnected sensor and data networks to collect data needed to inform a response through contextualization of the bio-event.
- **Analytics** - Exploit interconnected networks for biosurveillance, develop near real-time data analysis and visualization to inform decision makers, transform the data to knowledge that informs decision making.
- **Demonstrations** – Show reduced time to inform responses by decision makers.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Requirements				
Select sites for joint operational demonstrations and exercises with DOD to inform data needs.	Complete a biosurveillance technologies assessment. Complete a tailored risk assessment for biosurveillance activities. Determine the decision makers' biosurveillance information needs.	Complete a requirements assessment based on operational testing and end users' best practices.		
Objective: Integration				
Deliver an architecture framework for a national biosurveillance system that integrates government and commercial networks.	Deliver a prototype architecture capable of fusing three to four data modalities for anomaly detection.	Evaluate alternative data sources (e.g., Internet of Things, social media, diagnostics).		
Objective: Analytics				
	Complete a study on uncertainty propagation in decision trees.	Demonstrate decision uncertainties and certainties using compiled data sets.	Transition data aggregation and visualization tools to end users.	
Objective: Demonstrations				
	Demonstrate enhanced environmental detection technologies.	Complete a laboratory demonstration of dual use sensor concepts for environmental threat detection. Complete a large scale demonstration of environmental sensor systems to evaluate their performance.	Complete an information fusion exercise for discerning and understanding two simultaneous unknown threats.	

APEX PROGRAMS CONTINUED

Apex Program – Screening at Speed

Vision – The aviation checkpoint of the future will efficiently detect threats to aviation security while minimizing inconveniences to passengers. Passengers will approach the checkpoint and be identified (eventually through biometrics) and assigned a risk level. The passenger will place their carry on items on a conveyer belt leading to an enhanced X ray device with automatic threat recognition software. The passenger will then walk through a screening portal with minimal divesture of carried items. The systems will be dynamically configured according to the passenger's risk level. A very small number of passengers will be diverted to secondary inspection where non-invasive techniques will be used to resolve alarms from the carry on inspection system or the screening portal. Transportation security officers at the checkpoint will spend less time searching complicated two dimensional images and more time observing and assisting passengers and resolving alarms identified by the automatic threat recognition software. In short, the Screening at Speed Apex program will enhance security, enhance efficiency, and improve passengers' experience.

Strategic Drivers Frequent and devastating attacks against U.S. commercial aviation and other domestic targets began in 1988 with the bombing of Pan Am Flight 103 over Lockerbie, Scotland. Since then, there have been at least 10 attempts to destroy aircraft with IEDs, five of which targeted U.S. aircraft or U.S.-bound aircraft. All but one of these five plans called for suicide bombers to smuggle IEDs through an aviation checkpoint. On September 9, 2014, the Under Secretary for Science and Technology testified before the House Committee on Homeland Security that "noninvasive screening at speed will provide for comprehensive threat protection while adapting security to the pace of life rather than life to security. Whether screening people, baggage or cargo, unobtrusive technologies and improved processes will enable the seamless detection of threats while respecting privacy, with minimal impact to the speed of travel and the pace of commerce." More specific strategic guidance comes from the 2013 HSARPA/TSA R&D Test and Evaluation Strategic Plan, which states that S&T should endeavor to "accelerate the process of delivering new capabilities to the user that improve effectiveness and efficiency" and "support risk-driven operations to provide effective and efficient security."

Description of Capabilities:

- **Carry-on Bag Screening** Develop enhanced Advanced Technology (AT/AT2) carry on bag screening systems with automatic threat recognition (ATR) capability. Develop new more capable carry on bag screening technologies capable of three dimensional imaging and improved material discrimination.
- **Passenger Screening** Enhance Advanced Imaging Technology (AIT) passenger screening capabilities to minimize divesture and remove the need to "stop and pose."
- **Secondary Screening** – Enhance secondary screening processes and technologies to detect a broader range of threats with greater certainty and a low false alarm rate.
- **Application Program Interfaces** Design a set of application program interfaces for checkpoint screening systems that enable implementation of TSA's risk based screening programs.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: Carry-on Bag Screening				
Conduct test and evaluation of a carry on bag screening system with 3-D imaging.	Develop an advanced "AT2" X ray prototype.	Enhance multi energy X ray systems.	Develop X ray systems with dynamically configurable detection thresholds.	Demonstrate a prototype with fully functional automatic threat detection software.
Objective: Passenger Screening				
Demonstrate the AIT K band with dynamic aperture and automatic threat detection.	Integrate "K" and "W" systems with auto threat detection.			Demonstrate walk through of an AIT prototype with automatic threat detection software.
Objective: Secondary Screening				
Demonstrate an electronic device scanning system.	Develop a coded aperture micro mass spectrometer (ETD) prototype.	Develop more efficient sampling techniques for explosive trace detection.	Release an enhanced trace library.	Develop a prototype for a non contact ETD system.
Objective: Application Program Interfaces				
	Draft application program interface requirements.	Demonstrate Security Technology Integrated Program (STIP)-compliant primary and secondary screening products.		Demonstrate a fully integrated checkpoint that can respond to external risk input.

APEX PROGRAMS CONTINUED

TECHNOLOGY ENGINES

Technology Engines

Vision - Technology Engines are centralized functions that will provide standardized services to all Apex projects and across S&T. They will tailor their work based on each Apex program's individual focus, as well as requirements and future concepts. Through input from S&T subject matter experts and technology developers, the Technology Engines will provide best practices, technical services, expertise, lessons learned, reusable products, and solutions for Apex programs and other projects and initiatives.

Strategic Drivers - S&T's five visionary goals coalesced both in the expanded Apex program and the stand up of the Technology Engines, which augment S&T core capabilities through the provision of cross cutting capabilities; identification of near-term technology solutions developed by external partners, including non-traditional performers; and delivery of program and technology analysis, knowledge products, and recommendations on the future of technological innovation.

Description of Capabilities:

- **Situational Awareness and Decision Support (SANDS)** - Establish standards, specifications, capabilities, and best practices that allow secure, compatible, and relevant information sharing across the HSE and assured, secure access to databases, knowledge bases, modeling and simulation tools, and shared situational awareness products.
- **Communication and Network Technologies (CNET)** - Provide Apex programs with integrated communications and networking solutions that ensure operability and interoperability across all network platforms, ensuring the efficient and effective exchange of voice, video, and data information.
- **Data Analytics (Big Data)** - Enable Apex programs to leverage emerging storage, security, computation, and analytics technologies to create information analysis and sharing capabilities and rapidly convert data to decisions for homeland security systems, missions, and operations.

Four additional Technology Engines are emerging as "start ups" for FY 2015: Human Systems, Identity Access and Management, Modeling and Simulation, and Manufacturing.

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: SANDS – Geospatial Analytics and Processing; Open Data Standards and Exchange; Information Sharing and Integration; System Architecture Interoperability Visualization; Decision Support Services; Interoperable Voice and Data Communications				
Stand up a fully functioning and integrated SANDS Engine. Define Apex SANDS decision support requirements for: 1) Real-time Biothreat Awareness 2) Border Situational Awareness System Architecture Interoperability Visualization: 1) Perform BSA SOA Awareness	Geospatial Analytics, Processing, and Visualization: 1) Identify operational and functional capabilities. 2) Assess satellite data availability tool. Open Data Standards and Exchange: Assess open standards for data and sensors. Information Sharing and Integration: Coordinate with the information sharing community for independent validation and verification of requirements and capabilities. System Architecture Interoperability Visualization: Determine Apex BSA enterprise integration requirements. Decision Support Services: Develop mutual aid resource access capabilities.	Define SANDS requirements for emerging Apex priorities.		

TECHNOLOGY ENGINES CONTINUED

Technology Engines

FY 2015	FY 2016	FY 2017	FY 2018	FY 2019
Objective: CNET – Interoperable Voice and Data Communications; Indoor Location and Communications; Public Safety Broadband Video Quality Applications and Services; Audio Quality for Public Safety; Land Mobile Radio Standards and Compliance; Wireless Infrastructure Modeling				
Stand up a fully functioning and integrated CNET Engine.	Interoperable Voice and Data Communications: Integrate LMR, commercial LTE networks, and the Nationwide Public Safety Broadband Network. Indoor Location and Communications: Develop a wearable heads up display with enhanced reality. Public Safety Broadband Video Quality Applications and Services: Develop accelerated quality platforms supporting large volume video applications. P25 Standards and Compliance: Deliver assessment program maximizing radio interoperability. Wireless Infrastructure Modeling: Guide utilization of public safety wireless.	Define CNET requirements for emerging Apex priorities.		
Objective: Data Analytics – S&T Data Analytics Lab; Exploratory Methodology Mapping (EMM); Rapid Experimentation, Prototypes and Pilots (Rapid); Assessment of Emerging Technologies (Emerging); Strategic Research and Development Engagement (Strategic)				
Server Multi-tenant, on-site facility EMM: Counter-proliferation, cyber crimes Rapid: Streaming data sets, Internet Protocol geocoding, entity resolution Emerging: Graph architectures, spark Strategic: Office of Science and Technology Policy, Berkeley AMPlab (Algorithms, Machines and People)	Server Multi-tenant, on-site facility EMM: Counter-proliferation, cyber crimes Rapid: Streaming data sets, internet Protocol geocoding, entity resolution Emerging: Graph architectures, spark Strategic: Office of Science and Technology Policy, Berkeley AMPlab (Algorithms, Machines and People)	EMM: Cyber analysts, biothreat assessment Rapid: Large-scale sensor streams, instrumenting the analyst Emerging: Personal assistants Strategic: International collaboration	Scale Single Memory Model, transition of lab operations to the gov cloud EMM: Disaster response in instrumented environments Rapid: Lambda architecture for targeting Emerging: Instrumented Environments and Objects	Mobile Distributed File System, hybrid commercial, gov cloud EMM: Cybersecurity analysis for hybrid cloud environments Rapid: Machine learning for human analysis Emerging: Mixed Reality Analytics

CONCLUSION

This strategic plan demonstrates the directorate's commitment to deliver effective and innovative insight, methods, and solutions for the critical needs of the HSE. Taking into consideration the ever-changing nature of threats, R&D advances, and stakeholder needs, S&T leadership considers this plan to be a living document. As a result, S&T will continuously monitor progress on efforts described within the plan and update it as needed. In conclusion, S&T believes that with sufficient resourcing, this strategic plan will enable us to continue building upon a distinguished track record of excellence in delivering results to our HSE end users.

Part IV

This page is intentionally left blank.

Homeland
Security

Science and Technology

#152 - Provide methodology and return on investment (ROI) analysis that S&T conducts to determine whether HSARPA funding is yielding the desired results.

Response: S&T has implemented in-depth data collection and an analytic approach to internal measures through the annual Portfolio Analysis and Review (PAR). The PAR considers the program/project alignment with key mission and visionary goals, budget, Integrated Product Teams (IPT) alignment, metrics & measures, milestones, risk, and major accomplishments. Using this rich dataset along with internal and external review empowers leadership with a greater understanding and capability for data-driven optimization of the portfolio to maximize return on investment (ROI). S&T continues to develop and improve the analytic analysis of the portfolio.

The PAR provides a holistic view and context for all investments, provides accountability and transparency to senior leadership and the program managers, supports decision making, captures key data and lessons learned, and reduces redundancy.

One measure of the PAR is to assist leadership in understanding ROI, considering R&D and Non-R&D investments across the Directorate. This is a process by which S&T measures metrics, technical aspects, program execution, and strategy moving forward. S&T broadly considers budget, people, and work in determining the optimal portfolio investment. PAR, along with the standard efforts examining budget and human resources, is just one of the tools used to establish a baseline, where yearly evaluations are made. Determining the return on investment consists of several courses of action, including ensuring mission capabilities are maintained, ensuring a balanced portfolio, and focusing on key partnerships and mission sets.

In addition to using the PAR to measure strategic alignment, the Executive Steering Committee oversees an independent technical assessment of all Apex Programs to measure programmatic execution. This assessment reviews the program's scope, schedule, risks and transition likelihood to establish a baseline for and continuous tracking of program health. With these assessments, S&T ensures that its Apex programs are using funding effectively and delivering expected results to customers, or otherwise make necessary adjustments to do so.

#153 - Please provide details on what S&T has accomplished through the Silicon Valley Office; including what it costs on a yearly basis to maintain the office (salaries, benefits, contractors, etc. the total cost) and how its effectiveness is measured.

Response: Since launching in December 2015, the Silicon Valley Innovation Program (SVIP) has had a number of key accomplishments and built traction both with the tech start-up community and internally within DHS. The publishing of the Innovation Other Transaction Solicitation marked the first time that DHS S&T has leveraged the Other Transaction Authority for a procurement focused on non-traditional contractors/technology start-ups. The SVIP engages a number of DHS operational components and critical infrastructure partners to understand and communicate their needs and technology gaps to the start-up community and work with them to decide which innovative startups to fund. The SVIP provides accelerated non-dilutive funding (up to $800k over 4 phases) for product development to address DHS's needs and provides test environments and pilot opportunities to selected companies. This engagement has led to the release of 6 specific topic calls addressing a range of Department and critical infrastructure objectives. In particular, the SVIP is currently addressing national security areas in counterterrorism, border security, and aviation security with 4 Customs and Border Protection (CBP) focused topics.

As of December 15, 2016, more than 110 applications have been received across all 6 topic calls, while 9 Phase I awards (with 4 more pending) and 3 follow-on Phase II awards have also been made. The SVIP has also built awareness with 1500+ startups, accelerators and venture capitalists through S&T-hosted outreach events (e.g. Homeland Security and Industry Days) as well as participation in panels, roundtables, conferences, and Startup Meet Ups. In order to appropriately measure effectiveness, the SVIP has put together strategic and implementation plans laying out key performance measures. In FY16, the SVIP had an operating budget of approximately $5.0M, including approximately $210k in Federal Salary/Benefits/Travel, approximately $970k in support contracts, and approximately $4.02M dedicated for research awards. The SVIP uses space in a U.S. Secret Service office in San Jose, CA, under the terms of a Memorandum of Understanding (MOU). There is no cost to S&T for use of this space.

FY16 Budget (including Federal Salary/Benefits/Travel)

	Budget
Management and Administration	
Federal Staff	
(Salary/Benefits/Travel)	$210,000
Total M&A:	$210,000
Research, Development and Innovation	
Support Contracts	$970,865
Research Awards	$4,029,135
Total RD&I:	$5,000,000

Silicon Valley Innovation Program Accomplishments as of 12/15/16

- **Innovation Other Transaction Solicitation (OTS) published in December 2015**
    - The Innovation OTS marked the first time that S&T has leveraged the Other Transaction Authority for a procurement focused on non-traditional contractors/technology start-ups and provided the umbrella solicitation for individual calls addressing specific requirements
    - 6 topic calls have been released under the Innovation OTS to date (4 in support of CBP requirements)
        - Internet of Things (IoT) Security (Closed 12/11/16)
        - (CBP) Small Unmanned Aircraft Systems (sUAS) Capabilities
        - (CBP) Enhancing CBP Airport Passenger Processing
        - (CBP) K9 Wearable Technologies
        - (CBP) Enhancements to the Global Travel Assessments System (GTAS)
        - Financial Services Cyber Security Active Defense
- **117 Applications received (112 Phase I; 5 Phase II)**
- **9 Phase I awards have been made**
    - 5 under the IoT Security topic call
    - 3 under the sUAS Capabilities topic call (supports CBP requirements)
    - 1 under the Enhancements to the GTAS topic call (supports CBP requirements)
    - Geographic breakdown of Portfolio Companies: 3 from Silicon Valley, 2 from Southern California, 1 each from Texas, Georgia, Massachusetts and Washington (state)
    - *Note: 4 additional Phase I awards are pending

Company	**Award Amount**	**Topic Call**	**Location**
Pulzze Systems Inc.	$200,000	IoT Security	Sunnyvale, CA
Machine-to-Machine Intelligence Corporation (M2Mi)	$74,925	IoT Security	Moffett Field, CA
Whitescope LLC	$200,000	IoT Security	Half Moon Bay, CA
Factom Inc.	$199,350	IoT Security	Austin, TX
Ionic Security	$119,250	IoT Security	Atlanta, GA
Echodyne Corporation	$118,721	sUAS Capabilities	Bellevue, WA
Goleta Star LLC	$200,000	sUAS Capabilities	Los Angeles, CA
Shield AI Inc.	$199,960	sUAS Capabilities	San Diego, CA
Tamr	$162,302	Enhancements to the GTAS	Cambridge, MA
Total:	**$1,474,508**		

- **3 IoT Security companies have been selected for a Phase II award following the successful completion of their Phase I work and a successful Phase II application and oral pitch** (*Note: the other 2 current Phase I IoT awardees applications for Phase II are under review)

Company	**Award Amount**	**Topic Call**	**Location**
Pulzze Systems Inc.	$200,000	IoT Security	Sunnyvale, CA
Machine-to-Machine Intelligence Corporation (M2Mi)	$199,500	IoT Security	Moffett Field, CA
Factom Inc.	$199,980	IoT Security	Austin, TX
Total:	**$599,480**		

- **S&T SVIP has built awareness with 1500+ startups, accelerators, and venture capitalists through S&T-hosted outreach events (e.g. Homeland Security and Industry Days) as well as participation in panels, roundtables, conferences and Startup Meet Ups**
  - Homeland Security Day   Customs and Border Protection   Silicon Valley, CA April 2016.
    - The SVIP received a lot of positive feedback from startups, investors and traditional entities after the event. Many of the startups that attended sent follow up notes thanking us for holding the event, noting that it was really great that DHS is taking an active role in reaching out to their community, asking for help, and being transparent and open to improving the way we can work with them. They were also very impressed at the breadth of DHS's mission and had no idea that even a single agency (CBP) did so much. This feedback validates our need to educate the community about who DHS is and what our challenges are.
    - Over 25 applications have been received in response to the CBP topic areas.
  - Homeland Security Day – Finance Sector Cybersecurity – Boston, MA – November 2016.
    - This was the SVIP's first event in Boston, helping to increase the reach of the program to the Boston tech community, while also providing a venue for attendees to hear directly from finance sector representatives and gain an understanding of DHS's relationship with the finance sector.
  - Speaking engagements: the SVIP tries to get the word out as much as possible, from widely-attended events like the RSA Conference to smaller, trade-specific forums and meet-ups with venture firms and accelerators (e.g., JetBlue Technology Ventures, Plug N'Play, etc.).
  - Targeted social media outreach.

Performance Measures

Short Term (FY16 & FY17)			
Measure	**Measure Type**	**Measure Description**	**Metric**
Outreach	Output	Ability to identify and educate startups, enhance awareness of DHS challenges	# startups attending SVIP events, # startups responding to SVIP solicitations, and # referrals of startup companies to SVIP
Influence	Outcome	Shape product development in companies to align with the needs of DHS operational components	Degree of product shaping relative to a set of product attributes
Leverage	Outcome	The "leverage" of DHS funds with private sector investment	Ratio between DHS investment and private sector investment
Speed	Output, Outcome, Impact	Streamline and accelerate the funding process to startups	# days between publishing a call, submission of applications, notification of funding selection, and OTA contract start date
Startup Success	Outcome, Impact	Success in developing product needed by DHS while surviving the commercial market	# startups that complete each phase, # startups that proceed to the next phase, and ultimately the # startups completing the program
Geographic Diversity	Output	Ensure diversity of innovation and support economic development throughout all U.S. regions	# startups per state and country submitting applications

Longer Term (2 – 3 years)			
Measure	**Measure Type**	**Measure Description**	**Metric**
Component Acquisition	Outcome	Ability to identify and educate startups, enhance awareness of DHS challenges	# startups DHS components onramp into programs of record or direct acquisition
Operational Enhancement	Outcome, Impact	Mission enhancement resulting from deployment of SVIP funded innovative technologies and solutions	Component defined improvements, generally operational effectiveness or efficiency (e.g. agent patrols more area in less time)
Valuation	Outcome, Impact	Startups achieve growth in valuation in investment rounds based upon successful execution of milestones	Percentage increase in valuation of a company's stock following initial SVIP funding

#154 - Please provide a break down on what S&T spends to fund COEs, along with a list of projects funded jointly with the operational components.

Response: Congress established the DHS-created university-based Centers of Excellence (COEs) in the Homeland Security Act of 2002, and provides a specific annual appropriation to enable the S&T Office of University Programs (OUP) to fund 10 COEs. OUP provides research funding for COEs in topical areas that are linked to the DHS missions. In FY 2016, total base grant funding for the COEs was S30,081,765. For each COE, DHS stakeholders develop research topics and questions relevant to their missions. OUP has established both contract (basic ordering agreements) and grant (cooperative agreements) mechanisms to enable DHS and other federal agencies to fund research at a COE within scope that addresses federal priorities. Funding from non-OUP sources (supplemental funds) totaled $16,631,714 in FY 2016. The Basic Ordering Agreements (BOAs) enable DHS to write task orders that will benefit DHS's missions, while the grant mechanisms enable research projects that do not have a pre-specified outcome. The BOAs and grants allow DHS and other federal agencies to jointly fund COE projects with OUP using their own funds. OUP provides the base funding for COE management, as well as most indirect costs, graduate students, and prior research on which supplemental studies are based.

The COEs are attractive to external funding sources because these affiliated costs are supported by OUP base funds, leaving operational components and others to pay only the marginal project costs. For example, in fiscal years 2014 through 2016, the Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California received over S5 million of BOA task orders and supplemental grant funds from DHS components for focused research, development and analysis. CREATE's reputation and OUP's funding vehicles will enable CREATE to continue its work for DHS years past the end of its grant performance period in FY 2017.

Attachment 2: FY16 COE funding breakdown

#155 - Please provide a list of explanation of the top 5, by total dollar value, big data projects funded by S&T and which components they are for.

Response: Big Data projects are managed by the HSARPA Data Analytics Engine and target the development of next generation computation and analytics capabilities for S&T Apex Programs and for homeland security applications in DHS components and the Homeland Security Enterprise. The top program investment areas for 2017 are:

1) DHS Social Media Screening and Vetting for USCIS, CBP, and TSA. DHS S&T is providing social media analytics technologies for use in USCIS Refugee, CBP ESTA visa waiver, and TSA credentialed population screening and vetting pilot operations at the direction of the DHS Social Media Task Force and with re-programmed funding provided by the U. S. Congress. FY16: $4.6 M.
2) Live Stream Media Exploitation Tool development for Law Enforcement in partnership with NYPD Counter-terrorism Division and NPPD Office of Infrastructure Protection Commercial Facilities Sector. With increasing terrorist and criminal use of live streaming social media technology to expand the impact and/or establish command and control comes an urgent need to develop tools for law enforcement to exploit and counter these communications. FY16: ~$200k.
3) ICE Big Data Environment analytics for Homeland Security Investigations supporting ICE enforcement domains and with emerging applications for DNDO to meet requirements for the next generation Global Nuclear Detection Architecture, including advanced analysis of technology import data sources. FY16: $1.9 M.
4) Computation and analytics research and development support to the DHS S&T Border Situation Awareness, Next Generation First Responder and Real-time Bio-threat Assessment APEX programs. Moving public safety, border and bio-surveillance analytics to the cloud. Developing next generation real-time analytics for metro-scale, multi-party, multi-latency data networks. FY16: $1.6M.
5) Data Analytics Consulting for the re-design and implementation of the FEMA U. S. Fire Administration National Fire Incident Reporting System including fire service cloud analytics engagements with Chicago, Los Angeles, and NY Fire Departments. FY16: $100k.

#158 - Please provide the status of the DHS wholly owned laboratories, including those under construction, and the measures used to determine effectiveness.

Response:

Chemical Security Analysis Center

The Chemical Security Analysis Center's (CSAC) scientific and technical activities provide analysis and scientific assessment of the current and evolving chemical threat against the American homeland. This expertise includes basic chemical sciences related to chemical threats, hazard and risk analysis, and chemical threat characterization. CSAC currently maintains a high level of readiness.

CSAC is ISO 9001 complaint for all of our technical and business processes. CSAC maintains all of the necessary certifications to operate a DHS and DIA certified SCIF, as well as the certifications for operating the JWICS and HSDN computer networks within the SCIF. All are current.

National Biodefense Analysis and Countermeasures Center

National Biodefense Analysis and Countermeasures Center (NBACC) is a Federally Funded Research and Development Center (FFRDC) formed by DHS in 2006 that is operated and managed by the Battelle National Biodefense Institute, LLC (BNBI). The NBACC operations and management contract has been competed twice (2006 and 2015) with BNBI being selected both times. A documented process is used for NBACC strategic planning, annual planning, and the flow of requirements and priorities from DHS to the NBACC FFRDC. A DHS-approved Quality Assurance Surveillance Plan is utilized to assess performance multiple times each program year.

The NBACC is mission ready, addressing requirements identified in presidential directives, legislation, and national planning documents and guidance. The NBACC mission is to provide the scientific basis for characterization of biological threats and bioforensic analysis to support attribution of their planned or actual use. NBACC provides 24x7 operational support to federal law enforcement investigations and key scientific information for planning and responding to traditional and emerging biological threats.

NBACC has all required registrations and certifications required to meet mission goals. These include Biological Select Agents and Toxin registrations with the CDC and USDA for biosafety levels 2, 3 and 4 (4 being the highest level available). In FY16, NBACC has successfully renewed registrations with AAALAC International (animal care) and A2LA (ISO 17025).

National Biological and Agro-Defense Facility – Construction Project

The National Bio and Agro-Defense Facility (NBAF) mission will be to provide an enduring capability to enable the United States to conduct comprehensive research, develop vaccines, and provide enhanced diagnostic capabilities to protect against foreign animal, emerging, and zoonotic diseases that threaten our nation's food supply, agricultural economy, and public health. NBAF will ultimately replace Plum Island Animal Disease Center (PIADC) and all of its essential functions as well as provide additional capabilities for early development of medical countermeasures and the study of zoonotic diseases that affect livestock and other large animals.

NBAF will be located on the campus of Kansas State University (KSU) in Manhattan, Kansas. Based on the current schedule, construction activities will be completed in December 2020, facility commissioning activities will be completed in May 2021, select agent registration will be achieved in December 2022, and the mission will transition from Plum Island in 2023.

The National Bio and Agro-Defense Facility (NBAF) Acquisition Project is a Level 1 DHS Acquisition currently under construction in Manhattan, Kansas. The $1.25B cost baseline includes the planning, design, construction, and commissioning of the facility. To date, S222M worth of construction has been completed on schedule and on budget, and the project is on schedule to meet the established schedule baseline of a May 2021 completion. Considering all planning, design, and construction effort performed to date, the project is 35% complete.

National Urban Security Technology Laboratory

Located in New York City, the National Urban Security Technology Laboratory (NUSTL) is the only national laboratory focused exclusively on supporting state and local first responders capabilities to address the homeland security mission. The Lab provides First Responders the necessary services, products, and tools to prevent, protect against, mitigate, respond to, and recover from homeland security threats and events. More specifically, the Lab is mission ready to support the national first responder community by: by: 1) Conducting test & evaluation of First Responder technologies and systems, 2) Advising first responders on homeland security-related technology solutions and use, and 3) Developing science and technology-based solutions for response and recovery from a radiological/nuclear incident. NUSTL manages its performance and progress through its key performance parameters (KPPs) which specify performance goals on the Lab's operations, services and products. The Lab ensures KPPs are met through its Quality Management System (QMS) and Safety Health and Environmental Management System (SHEMS) which are compliant with International Standards Organization (ISO) 9001:2015 Quality Management, ISO-14001 Environmental Management and American National Standards Institute Occupational Health and Safety standards. These management systems have been found to be highly efficient, effective and suitable by external auditors. In 2016, the Lab's QMS received a near flawless audit score with the laboratory meeting 176 out of 182 requirements met, a 96.7% conformance. Also in 2016, the laboratory's SHEMS was rated highly effective and was noted as the benchmark in which all labs should follow.

Plum Island Animal Disease Center

The PIADC mission is to protect the nation's livestock from foreign animal diseases. PIADC is mission ready to provide diagnostic support services and also provide research support with the exception of using livestock for vaccine and diagnostic testing. Currently, the laboratory's liquid waste decontamination plant has limitations on the amount of liquid waste it can heat treat and this prevents the use of livestock for research as the current plant cannot support this additional waste stream.

To ensure mission readiness until NBAF comes on-line in 2022, targeted sustainment projects valued collectively at approximately $10.2M include the installation of two new water wells, replacement of an exit autoclave, salt water system modifications, and bio containment ventilation and building management enhancements. All projects are currently anticipated to be completed by FY 18.

PIADC is registered for select agents with the USDA and is a tier one level 5 security lab. The operations and maintenance contractor is ISO9001 registered for higher risk service activities.

Transportation Security Laboratory

The Department of Homeland Security's Transportation Security Laboratory (TSL) performs test and evaluation of explosives detection technologies to support Transportation Security Administration (TSA) and other DHS acquisition efforts. All explosives detection screening equipment currently used by TSA at US airports has been rigorously tested and formally certified by the TSL. The TSL also works directly with systems developers to ensure fast and efficient transition of emerging technologies to TSA and other public and private Homeland Security Enterprise (HSE) agents.

The TSL is fully operational and is meeting its mission to test the explosives detection performance of screening equipment used at all U.S. airports. The TSL measures its productivity by examining the cost and duration of Test and Evaluation (T&E) activities.

The current construction plan is to apply $27.5 million in FY18/19 to expand physics and chemistry laboratories to enable more efficient and comprehensive testing of explosive detection devices required by the Homeland Security Enterprise.

The TSL maintains ISO 9000 and ISO 17025 certification through yearly audits, maintains a license with the Nuclear Regulatory Commission for operation of X-ray based detection and analytical equipment, and provides the Bureau of Alcohol, Tobacco and Firearms (ATF) with annual summaries of the Lab's explosives and weapons inventories and operations.

COE	Total FY16 OUP Funding
Center for Awareness and Localization of Explosives-Related Threats (ALERT)	$ 3,876,163.00
Center for Border, Trade, Immigration Research (CBTIR)	$ 3,600,000.00
Cross-Border Threats Screening and Supply Chain Defense (CBTS)**	$ 200,000.00
Center for Homeland Security Qualitative Analysis (CHSQA)**	$ 250,000.00
Center for Criminal Investigations and Network Analysis (CINA)**	$ 250,000.00
Criticial Infrastructure Resilience Institute (CIRI)	$ 3,762,845.39
Coastal Resilience Center (CRC)	$ 3,840,000.00
Center for Risk and Economic Analysis of Terrorism Events (CREATE)**	$ 1,520,000.00
Center for Visualization and Data Analystics (CVADA)**	$ 1,530,000.00
Food Protections Defense Institute (FPDI)**	$ 1,302,778.00
Maritime Security Center / Arctic Domain Awareness Center (MSC/ADAC)	$ 4,600,000.00
National Consortium for the Study of Terrorism and Responses to Terrorism (START)	$ 3,600,000.00
Training Institute for Qualitative Analysis (TIQA)*	$ 350,000.00
National Center for Zoonotic and Animal Disease Defense (ZADD)**	$ 1,399,979.00
Total	**$ 30,081,765.39**

* Training institute, not a COE

** COE starting or ending, partial-year funding

Fiscal Year 2016

Sum of Amount Invested	Column Labels		
Row Labels	BOA	Coop	Grand Total
DHS CBP	**750000**		**750000**
DHS DNDO	**1154698.38**		**1154698.38**
DHS I&A		$ 10,000.00	$ 10,000.00
DHS OHA	$ 726,781.40		$ 726,781.40
DHS TSA	$ 179,246.40		$ 179,246.40
DOD		$ 1,953,750.00	$ 1,953,750.00
NCTC		$ 499,978.00	$ 499,978.00
S&T CDS	$ 3,547,000.00		$ 3,547,000.00
S&T FRG	$ 1,995,000.00	$ 265,000.00	$ 2,260,000.00
S&T HSARPA CBD	$ 659,515.00	$ 582,201.00	$ 1,241,716.00
S&T HSARPA CSD	$ 1,200,000.00	$ 100,000.00	$ 1,300,000.00
S&T HSARPA EXD	$ 1,234,221.00	$ 1,324,323.01	$ 2,558,544.01
S&T OSAI		$ 450,000.00	$ 450,000.00
Grand Total	$ 11,446,462.18	$ 5,185,252.01	$ 16,631,714.19

Center of Excellence	Investing Organization	Amount Invested	Funding Vehicle	Project Name / Description
CREATE	DHS CBP	$ 750,000.00	BDA	Perform a study to recomend improvements to CBP's strategic resource assessment process
START	DHS DNDO	$ 23,000.00	BOA	South and Central Asia Architecture Analysis
5TART	DHS DNDD	$ 707,698.38	BDA	Developing integrated radiological and nuclear detection architecture for the interior and internation mission space
START	DHS DNDO	$ 424,000.00	BOA	Developing and Validating an International Commercial Air Cargo Insider Threat Tool
5TART	DHS I&A	$ 10,000.00	Coop	Scientific Method Development to Limit Chemical and Biological Weapons Threat 5pace
FPDI	DHS OHA	$ 139,206.40	BOA	ICLN Web Portal
ZADD	DHS OHA	$ 254,457.00	BDA	Analysis of Chagas disease epidemiology in working dogs
ZADD	DHS OHA	$ 333,118.00	BOA	Initial structure and capability of National Livestock Readiness Program
NTSCOE	DHS TSA	$ 146,752.00	BOA	
5TART	DHS T5A	$ 32,494.40	BDA	Seminar Series for TSA
START	DOD	$ 214,750.00	Coop	SMA EUCOM Support: Threats and Opportunities for Conflict and Cooperation within Eurasia
START	DOD	$ 245,000.00	Coop	SMA EUCOM Support: Timed Influence Net (TIN) Model
START	DOD	$ 544,848.00	Coop	SMA Support to SOCCENT
START	DOD	$ 949,152.00	Coop	EUCOM Gray Zone
START	NCTC	$ 499,978.00	Coop	ICONS Project
MSC	S&T CDS	$ 597,000.00	BDA	Counter Unmanned Aerial Systems
MSC	S&T CDS	$ 2,950,000.00	BOA	Counter Unmanned Aerial Systems
CVADA	S&T FRG	$ 1,995,000.00	BDA	ICIF and Project Interoperability 2.0 Project
START	S&T FRG	$ 265,000.00	Coop	Supplemental funding for TEVUS and PIRUS projects added to continuation funding
START	S&T HSARPA CBD	$ 10,000.00	Coop	Scientific Method Development to Limit Chemical and Biological Weapons Threat Space
START	S&T HSARPA CBD	$ 274,496.00	Coop	Profiling the Chemical Biological Adversary
START	S&T HSARPA CBD	$ 297,705.00	Coop	CBD Division Strategy Development
ZADD	S&T HSARPA CBD	$ 259,935.00	BOA	VECTOR-BORNE VIRUSES REPOSITORY MATERIALS FOR PUBLIC HEALTH ACTIDNABLE ASSAY (PHAA) VALIDATION
ZADD	S&T HSARPA CBD	$ 399,580.00	BDA	AGConnect APEX Integration Effort
CVADA	S&T HSARPA CSD	$ 1,200,000.00	BDA	Identity Management and Data Privacy
FPDI	S&T HSARPA CSD	$ 100,000.00	Coop	Cyber Food Project
ALERT	S&T HSARPA EXD	$ 75,000.00	Coop	Improvised Explosives Trace Analysis and Mass Transfer (vapor characterization and signature study of selected Homemade Explosives (HMEs)
ALERT	S&T HSARPA EXD	$ 99,377.01	Coop	NYPD Counter Terrorism Division
ALERT	S&T HSARPA EXD	$ 950,000.00	Coop	Develop alorithmic methods for tracking passenger travel at airports
ALERT	S&T HSARPA EXD	$ 99,946.00	Coop	Test and Evaluation with the NYPD Counterterrorism Dept
ALERT	S&T HSARPA EXD	$ 100,000.00	Coop	Equipment Test and Evaluation with the Boston Police Department (BPD), Boston Fire Department (BFD), the Boston Emergency Services Unit (ESU) and Fenway Park Personnel
ALERT	S&T HSARPA EXD	$ 1,234,221.00	BOA	Research and Development of Algorithms for Improved Image Quality for Checkpoint Explosive Detection Systems

CVADA	S&T OSAI	$ 450,000.00	Coop	Economics Security Project
		$ 16,631,714.19		

Integrated Product Teams for Department of Homeland Security R&D

FY16 Report

Homeland
Security

To be quicker, smarter, and more adaptable to all hazards, the Department of Homeland Security (DHS) relies on innovative and effective technologies. As a result, our approach to research and development (R&D) must support identifying and implementing the best solutions for the homeland security enterprise. This is a complex but necessary endeavor that keeps our field personnel safe while also protecting our homeland.

To ensure this is happening in the most efficient and effective way across the Department, I signed a memo in August 2015 re-establishing integrated product teams (IPTs) to coordinate R&D efforts across DHS. The initial IPTs covered the following mission areas: Aviation Security, Biological Threat, Counterterrorism, Border Security, and Cyber Security.

The IPTs brought together some of the best operational and technical minds in the Department, and the governance structure established for the IPTs truly embraced a culture of collaboration. Drawing on expertise resident in the IPTs, sub-IPTs, and the Science and Technology Research Council, the IPT process compiled information on R&D activities across DHS in a way that was unprecedented until now. This information provides an invaluable tool for DHS as we work together to manage our vast mission space and make wise technological investments.

This report describes the structure, methodology, and results of the fiscal year 2016 (FY16) IPT process. In my August 2015 memo, I directed the IPTs to identify 1) ongoing R&D activities across the Department; and 2) high-priority capability gaps and corresponding technology solutions. The DHS Science and Technology Directorate compiled and submitted this information to me earlier this year. Due to the sensitive nature of the homeland security mission, this information must be protected from broad public release. As a result, this report does not include all the supporting information generated through the FY16 IPT process but it does inform the public of the important work being done by the IPTs to coordinate DHS R&D activities to address priority homeland security needs.

In years to come, the structure that the IPTs bring to DHS R&D efforts will continue to identify effective and innovative solutions to address the most pressing challenges facing the homeland.

Sincerely,

Jeh Charles Johnson

Table of Contents

Executive Summary

As the homeland security mission continues to evolve, the Department of Homeland Security (DHS) must focus its research and development (R&D) efforts to develop technology solutions that address the most critical needs. The breadth and complexity of the DHS mission space pose challenges for tracking all ongoing R&D efforts and aligning those efforts to Department goals and priorities. In late 2012, the Government Accountability Office (GAO) recommended that DHS develop policies for coordinating R&D activities and establish a mechanism for tracking R&D projects. The DHS Science and Technology Directorate (S&T) worked with other DHS components to improve R&D tracking and coordination, including issuing a DHS Directive and Instruction that provide definitions for R&D and establish policies for coordinating R&D activities across the Department.

To reinforce these ongoing efforts, the Secretary of Homeland Security issued a memorandum in August 2015 directing S&T to establish Integrated Product Teams (IPTs) to identify and coordinate DHS R&D efforts in priority mission areas. The initial IPTs covered the following DHS missions: Aviation Security, Biological Threat, Counterterrorism, Border Security, and Cyber Security. In response to the Secretary's direction, S&T established an operational framework and process to support the stand-up, governance, and ongoing operations of the IPTs. The IPTs are explicitly linked to the work of the DHS Joint Requirements Council (JRC) and will serve as the central mechanism by which the Department identifies technological capability gaps and coordinates R&D efforts to close those gaps. The level of direct interaction between the IPTs and the JRC will increase over time as both processes evolve and the JRC processes for joint assessment of requirements and operational capability gap prioritization continue to mature.

The IPT process facilitates improved R&D coordination by:

- Promulgating a standardized approach for identifying and tracking DHS R&D efforts, thereby addressing GAO's recommendations to improve R&D coordination across the Department;
- Establishing a common mechanism and procedures for gathering and reporting priority gaps and corresponding R&D efforts to develop solutions;
- Providing a technology review platform to identify and mitigate duplicative and overlapping R&D efforts within DHS; and
- Helping to fulfill longstanding statutory requirements for DHS and S&T to align Departmental R&D efforts with DHS acquisitions.

The IPT process was designed to be a truly collaborative, cross-component endeavor. While S&T is responsible for leading the overall effort, the individual IPTs were led by senior executives from DHS components, with representatives of the JRC participating at various levels. In this way, the IPT process supports and strengthens the Department's Unity of Effort Initiative. Table ES-1 shows the component leads and members of the fiscal year 2016 (FY16) IPTs and sub-IPTs.

IPT Name	Component IPT Chairs/Co-Chairs	Component Membership
Aviation Security	TSA	CBP, DNDO, NPPD, USCG, USSS
Biological Threat	FEMA and OHA	CBP, MGMT, NPPD, TSA, USCG, USSS
Border Security	CBP	DNDO, ICE, USCG
Counterterrorism	I&A	CBP, DNDO, ICE, NPPD, TSA, USCG, USSS
Cybersecurity	NPPD and MGMT/CISO	CBP, CRCL, FEMA, I&A, ICE, PLCY, Privacy, TSA, USCG, USCIS, USSS

Table ES-1. Component Representation on the IPTs and Sub-IPTs

The IPT process established for FY16 included three main implementing bodies—sub-IPTs, IPTs, and the S&T Research Council (SRC)—plus an advisory body, as illustrated in Figure ES-1. The IPT process informed products that were provided to the Under Secretary of S&T (USST) for review and ultimate delivery to the Secretary of Homeland Security.

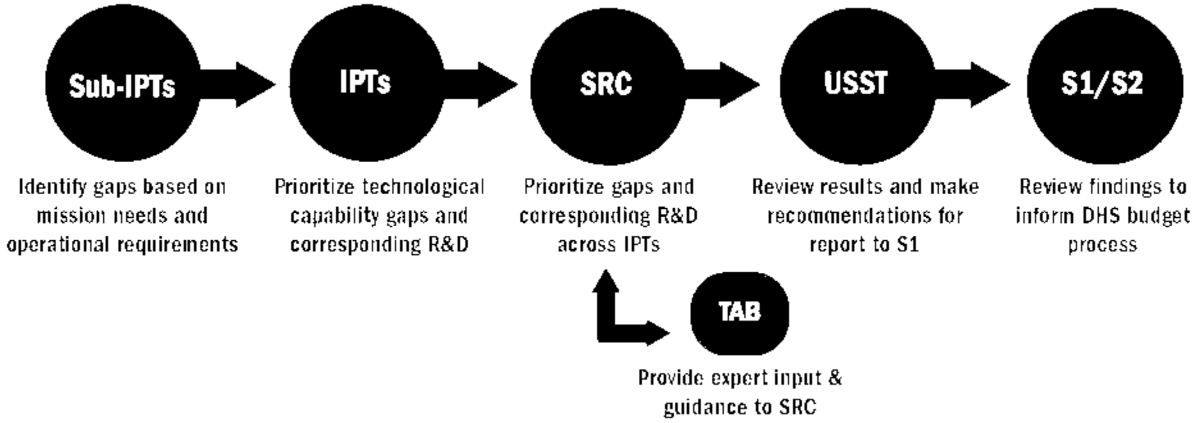

Sub-IPTs
IPTs
SRC
USST
S1/S2
Identify gaps based on mission needs and operational requirements
Prioritize technological capability gaps and corresponding R&D
Prioritize gaps and corresponding R&D across IPTs
Review results and make recommendations for report to S1
Review findings to inform DHS budget process
TAB
Provide expert input & guidance to SRC

Figure ES-1. IPT Governance Structure

The sub-IPTs included component and S&T representatives with expertise in specific topical areas within the broader mission area of each IPT. JRC representatives also participated in the sub-IPTs to ensure alignment with the JRC process and the consideration of operational capability gaps at the sub-IPT level. IPTs consolidated the gaps identified by their sub-IPTs and determined the top high-priority technological capability gaps within their IPT mission areas.

During the FY16 cycle, the SRC included the senior component leads of the IPTs, a senior representative of the JRC, and a chair from S&T. To ensure broad unity of effort, the SRC convened a Technical Advisory Board (TAB) consisting of senior representatives from DHS HQ offices that were not represented on the IPTs. The TAB reviewed and provided expert input on SRC recommendations and draft products. The SRC reviewed the top-priority gaps from four of the five IPTs[1] and then voted to identify the highest-priority gaps across the IPTs.

The highest-priority DHS technological capability gaps identified in FY16 are listed in Table ES-2.

[1] *Due to time limitations during the FY16 cycle, the SRC identified high-priority technological capability gaps across four of the five IPTs.*

IPT	Technological Capability Gap
Aviation Security	Capability to accurately identify and screen checked baggage based on the owners Passenger Clearance Ranking
	Capability to verify a passenger's identification
	Enhanced ability to conduct primary screening of passengers in aviation security screening checkpoints (currently performed by advanced imaging technology and walk-through metal detectors) that provides the ability to distinguish threats from non-threats that are placed on the body
	Enhanced risk-based screening algorithms development for security technology to support operator and associated policy decisions
	Improved capability to allow operators to screen passengers' carry on and checked bags for prohibited items to protect against sophisticated IED attacks (various explosive types)
	Improvement needed for screening methods against attacks using cargo IED, one or more, when in flight (various explosives types)
Biological Threat	Compact Personal Protective Equipment (PPE): Emergency/Escape Hood
	Decision Support for Operational Decision Making, including PPE use
	Means for field agents to detect, identify and classify the presence of biological agents
	Biological dispersion event modeling
	Data assimilation and predictive analysis to inform decision making in the field and operations centers
	Advances to allow for better timeliness to verify a biological attack
Border Security	Biometric Entry and Exit (counting and measuring)
	Improve performance of non-intrusive inspection (NII) detectors and/or sources
	Small Dark Aircraft Detection and Timely Interdiction
	Sensor and Intelligence Information Sharing and Data Analytics
	Land/In-Between Ports-of-Entry Situational Awareness
	Tunnel Detection, Surveillance, and Forensics
	Maritime Surveillance and Communications in Remote Environments
	Small Dark Vessel Detection
Cybersecurity	Distributed Cloud-Based Communications and Monitoring
	ICS Control Systems, Cyber Sensors, Analytics, and Prevention Capabilities
	Method for forensic examiners to capture user data from networked devices (the "Internet of Things")
	Lack of cybersecurity effectiveness, severity, and comparative metrics

Table ES-2. Highest-Priority Gaps Resulting from the FY16 IPT Process

The Secretary also charged the IPTs with identifying R&D activities being performed across DHS. The sub-IPTs and IPTs documented R&D efforts as they worked to identify priority capability gaps within their mission areas. In addition, S&T initiated a data call to all DHS components requesting information on ongoing research and/or development activities. The information compiled through these efforts represents the *Report of Coordinated DHS R&D*, which S&T delivered to the Secretary in March 2016, in accordance with the August 2015 memorandum.

The IPTs then identified R&D efforts that addressed the high-priority gaps. The SRC reviewed these R&D efforts and recommended ongoing analysis of the technical solutions for high-priority gaps. The SRC also recommended that additional or new R&D be considered for high-priority gaps with insufficient or no associated R&D. The identified high-priority gaps and the R&D efforts that address those gaps are captured in the *High-Priority Technology Solutions* document, which S&T also delivered to the Secretary in March 2016.

The results of the FY16 IPT process will inform a DHS acquisition profile aligned to the highest-priority gaps, thus providing a blueprint that will support a common appropriations structure to Congress. This will ultimately lead to full transparency of R&D activities and benchmark the necessary steps for producing a comprehensive and integrated DHS-wide acquisition program for R&D.

IPTs In Action

During the Bio Threat sub-IPT meetings on Detect, Identify and/or Classify, representatives from CBP, FEMA, and USSS identified the requirement for rapid warning, identification, and characterization of biological threats. While these components would field such technology for differing uses, including force protection, public safety, and decision support, the Bio Threat IPT chose to consolidate these otherwise independent requirements into joint projects. This resulted in improved communication among components and a more focused R&D acquisition profile.

The IPTs worked closely with legal, policy, civil liberties, and privacy advisors to ensure that appropriate protections were built into planned outcomes and issues were addressed through review and adjudication cycles.

The IPT process established for the FY16 cycle is both repeatable and flexible and provides a strong foundation for future evolution of the process. To enhance future iterations of the IPT process, an independent after-action review will follow each annual cycle to identify lessons learned and recommend process improvements for implementation in future years.

Perhaps most important, the IPT process facilitates cross-Department collaboration. Executives from across DHS now have an established mechanism for coordinating and prioritizing R&D activities that will result in effective solutions for near- and longer-term mission challenges.

I. Introduction

The Department of Homeland Security (DHS) relies on innovative and effective technology solutions to address the priority needs of the homeland security enterprise (HSE). Title III of the Homeland Security Act of 2002, as amended, gives the Under Secretary for Science and Technology the responsibility for identifying priorities and coordinating research and development (R&D) activities in support of the Department's mission.

The size and scope of the homeland security mission make it difficult to track all R&D efforts across DHS and align those efforts to Department goals and priorities. In 2012, the Government Accountability Office (GAO) recommended that DHS establish policies and guidance for defining, reporting, and coordinating R&D efforts across the Department. The DHS Science and Technology Directorate (S&T) worked with other DHS components to improve R&D coordination through various means, including developing a DHS Directive and Instruction that define R&D and establish policies for identifying and reporting R&D activities.

Building on the efforts to date, the Secretary of Homeland Security issued a memorandum in August 2015 establishing Integrated Product Teams (IPTs) as the central mechanism by which DHS identifies and coordinates its R&D efforts in priority mission areas. The initial IPTs focused on the following DHS missions: Aviation Security, Biological Threat, Counterterrorism, Border Security, and Cyber Security. Supporting the broader Unity of Effort Initiative, the IPTs brought together cross-component teams to align the Department's R&D investments with priority technological capability gaps. While S&T was charged with leading the overall effort, the individual IPTs were led by senior representatives of the components. Subject matter experts from the DHS Joint Requirements Council (JRC) also participated at various levels. Figure 1 illustrates the cross-component collaboration and unity of effort inherent in the IPT process.

In addition to the five IPTs established for fiscal year 2016 (FY16), S&T continues to support the First Responder Resource Group (FRRG), a working group that helps to identify the priority needs of State and local responders in the field, as well as the Domestic Nuclear Detection Office (DNDO). Given the breadth and depth of DHS mission space and the associated R&D needs, the IPT process will continue to be refined to meet the most pressing homeland security demands.

The FY16 IPTs identified technological capability gaps to gain a better understanding of current and emerging R&D needs. The IPTs then identified R&D efforts to develop solutions that address the most critical gaps to support the security and resilience of the Nation.

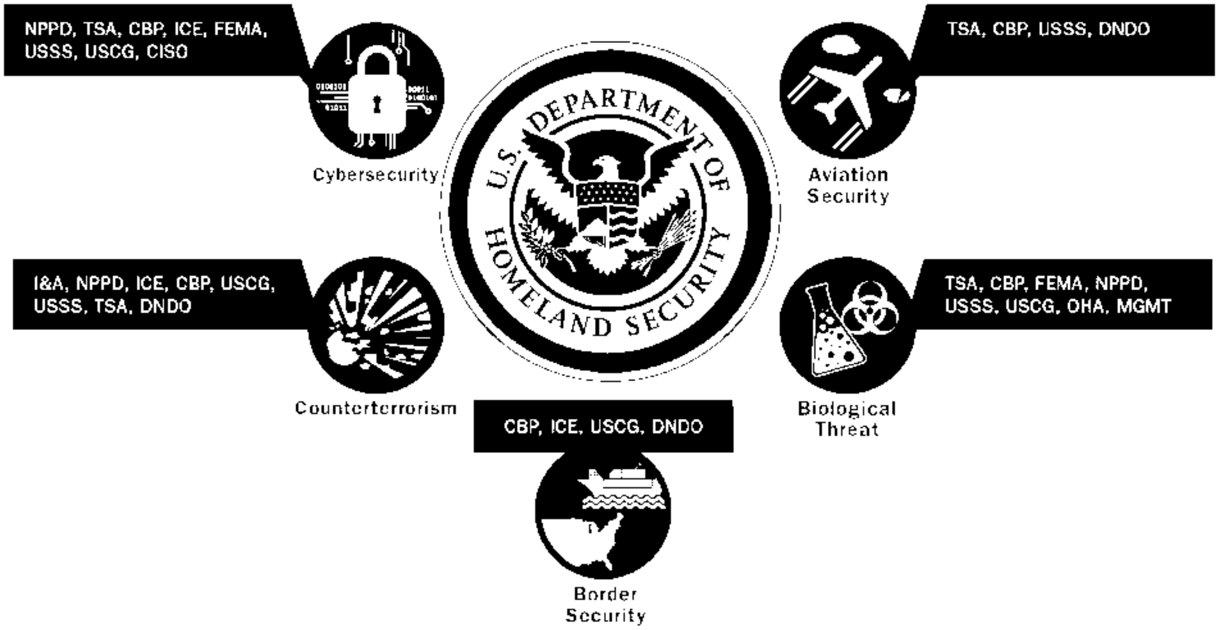

NPPD, TSA, CBP, ICE, FEMA, USSS, USCG, CISO
Cybersecurity
TSA, CBP, USSS, DNDO
Aviation Security
I&A, NPPD, ICE, CBP, USCG, USSS, TSA, DNDO
Counterterrorism
TSA, CBP, FEMA, NPPD, USSS, USCG, OHA, MGMT
Biological Threat
CBP, ICE, USCG, DNDO
Border Security

Figure 1. Integrated Product Teams Unity of Effort

The results of the FY16 IPT process informed the following two products identified in the Secretary's August 2015 memo:

- The *Report of Coordinated DHS R&D*, which captures ongoing DHS R&D activities.
- The *High-Priority Technology Solutions* document, which captures high-priority gaps and the R&D efforts to develop solutions that address those gaps.

The outcomes of the IPT process outlined in this report will focus DHS R&D to reflect the evolving landscape of homeland security threats and hazards. By identifying R&D efforts that address high-priority gaps, the component-driven IPT process will influence resource allocation for DHS R&D activities.

II. Goals and Objectives

While many DHS components provide methods and solutions to address homeland security challenges, previous efforts to coordinate DHS R&D activities were limited to ad hoc arrangements that were not necessarily aligned to specific mission areas or component acquisitions. Within DHS, only DNDO, the United States Coast Guard (USCG), and the S&T Directorate are granted R&D responsibilities by law. Other DHS components may pursue and conduct their own R&D, so long as those activities are coordinated through S&T. As responsible stewards of taxpayer dollars, DHS has made it a priority to identify and coordinate R&D efforts across the Department to ensure mission alignment and the proper use of Federal Government appropriations.

Going forward, the IPT process can assist the Department in prioritizing its essential R&D programs and core capabilities, which will ultimately lead to a traceable and executable DHS R&D plan. From a funding perspective, IPTs provide information that supports the development of a DHS acquisition profile that aligns to the highest-priority gaps, thus providing a blueprint that will support a common appropriations structure to Congress. Most important, the IPT process facilitates broad collaboration across DHS components, opening new channels for executives to discuss and coordinate R&D activities to address the highest-priority needs of their operational staff.

The Secretary outlined five objectives for the IPTs (presented in the box on the right), which provide a roadmap for achieving the overall goal of the effort. They are designed to promote understanding of the Department's most pressing R&D needs and how best to meet those needs. These objectives foster transparency and collaboration to validate technology solutions and leverage R&D investments for the greatest benefit to DHS missions.

The IPT process was designed to achieve each of these objectives and will help to address the GAO recommendations to improve coordination of DHS R&D activities.

While delivery of the two documents identified in the August 2015 memo addresses the first two objectives, the IPT process established for FY16 provides the foundation to achieve the remaining three objectives in future annual **cycles**.

Overall Goal of IPT Effort

Coordinate DHS-wide R&D to address priority missions.

Objectives for the IPTs

Identify and prioritize DHS technological capability gaps and corresponding solutions to close those gaps.

Identify R&D work being performed across DHS, both in traditional R&D funding lines and that occurring within component acquisition programs.

Ensure technology being acquired will meet DHS and component mission needs.

Identify and de-conflict duplicative R&D efforts.

Develop and report metrics for the transition of technological solutions to close capability gaps.

III. Integrated Product Team Process

In response to the Secretary's direction, S&T established an organizational framework and functional process in FY16 to support the stand-up, governance, and ongoing operations of the IPTs. Figure 2 shows the governance structure and the main entities involved in implementing the IPT process. More details on the structure and functions of the IPT process are provided in Appendix A.

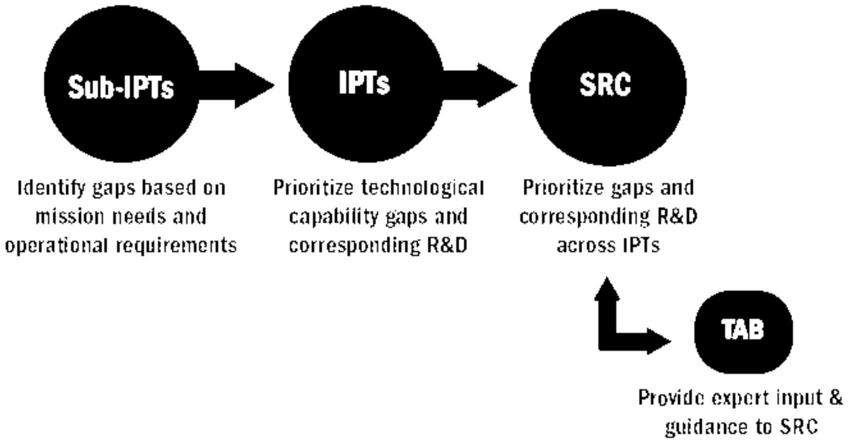

Sub-IPTs
IPTs
SRC
Identify gaps based on mission needs and operational requirements
Prioritize technological capability gaps and corresponding R&D
Prioritize gaps and corresponding R&D across IPTs
TAB
Provide expert input & guidance to SRC

Figure 2. IPT Governance Structure

Definition of R&D

For purposes of identifying R&D activities across DHS, the IPT process used the following definition of R&D:

- **Basic and applied research** includes systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and/or observable facts. The difference between basic and applied research is that basic research is normally conducted without specific applications toward processes or products in mind, while applied research is conducted to determine the means by which a recognized and specific operational need may be met.[2]
- **Development** is the systematic application of knowledge toward the production of useful materials, devices, and systems or methods that leverage the results of applied research activities. Development activities include the following: validation and demonstration of a chosen technology in laboratory, representative, and operational environments; improvement on research prototypes; integration into systems and subsystems; addressing manufacturing, producibility, and sustainability needs; and independent operational test and evaluation.[3]

[2] *Id.* Department of Homeland Security Instruction 069-02-001, Revision 01 (DRAFT), June 2016. See also Delegation to the Under Secretary for Science and Technology; Annex A, DHS Delegation 10001 Revision 1, April 28, 2014.

[3] *Id.*

IV. Technological Capability Gaps and Corresponding R&D

Technological Capability Gaps

In keeping with the Secretary's direction, the IPT effort engaged R&D stakeholders from across DHS in identifying technological capability gaps that impact priority homeland security missions. Knowledge of these gaps provides context for understanding ongoing and needed R&D activities across the DHS enterprise.

Sub-IPT and IPT Identification and Priority Ranking. IPTs were tasked with identifying technological capability gaps in need of research and/or development in their respective mission areas. The initial identification of gaps occurred at the sub-IPT level. To guide and structure this effort, S&T provided the sub-IPTs with a template for consistent data collection. The sub-IPTs ranked each of the identified gaps as a high, medium, or low priority for R&D-based capability development within their specific topic area.

Moving up one level, the IPTs performed a second round of priority ranking of identified gaps. Compiling the priority gaps from across their sub-IPTs, each IPT validated the lists and identified additional gaps as applicable. The IPTs then assigned a ranking of high, medium, or low priority to each gap on the list.

Real-world events in 2015 (i.e., the attacks in Paris and San Bernardino) delayed the establishment of the Counterterrorism (CT) IPT. As a result, the CT IPT did not submit gaps for consideration by the SRC in FY16, though some of the CT sub-IPTs did convene to identify priority gaps within their specific topic areas.

SRC Priority Ranking. The SRC performed the final priority ranking of gaps from each IPT that completed the process for FY16. As a result, the SRC voted on the high-priority gaps submitted by four of the five established IPTs. The SRC convened a meeting to review and discuss the top-priority gaps from each IPT to identify the gaps determined to be most important for DHS R&D investment. As part of the SRC voting process, each IPT chair presented the high-priority gaps nominated by his/her IPT and the SRC members voted to validate each gap as a high priority or re-designate it as medium or low. Through this process, the SRC identified a total of 24 high-priority technological capability gaps in need of research and/or development across the IPTs. General descriptions of the high-priority DHS technological capability gaps identified for FY16 are provided in Table 1.

IPT	Technological Capability Gap
Aviation Security	Capability to accurately identify and screen checked baggage based on the owners Passenger Clearance Ranking
	Capability to verify a passenger's identification
	Enhanced ability to conduct primary screening of passengers in aviation security screening checkpoints (currently performed by advanced imaging technology and walk-through metal detectors) that provides the ability to distinguish threats from non-threats that are placed on the body
	Enhanced risk-based screening algorithms development for security technology to support operator and associated policy decisions
	Improved capability to allow operators to screen passengers' carry-on and checked bags for prohibited items to protect against sophisticated IED attacks (various explosive types)
	Improvement needed for screening methods against attacks using cargo IED, one or more, when in flight (various explosives types)
Biological Threat	Compact Personal Protective Equipment PPE; Emergency/Escape Hood
	Decision Support for Operational Decision Making, including PPE use
	Means for field agents to detect, identify and classify the presence of biological agents
	Biological dispersion event modeling
	Data assimilation and predictive analysis to inform decision making in the field and operations centers
	Advances to allow for better timeliness to verify a biological attack
Border Security	Biometric Entry and Exit (counting and measuring)
	Improve performance of non-intrusive inspection (NII) detectors and/or sources
	Small Dark Aircraft Detection and Timely Interdiction
	Sensor and Intelligence Information Sharing and Data Analytics
	Land/In-Between Ports-of-Entry Situational Awareness
	Tunnel Detection, Surveillance, and Forensics
	Maritime Surveillance and Communications in Remote Environments
	Small Dark Vessel Detection
Cybersecurity	Distributed Cloud-Based Communications and Monitoring
	ICS Control Systems, Cyber Sensors, Analytics, and Prevention Capabilities
	Method for forensic examiners to capture user data from networked devices (the "Internet of Things")
	Lack of cybersecurity effectiveness, severity, and comparative metrics

Table 1. Highest-Priority Gaps Resulting from the FY16 IPT Process

The following section provides amplifying information about the gaps listed in Table 1. This includes a description of the relevant IPT mission area and the need(s) associated with each high-priority gap. Taken together, this information provides context to help industry and the public understand the Department's priority needs, which can lead to the identification of potential technology solutions that address our most pressing homeland security challenges.

Aviation Security: The aviation security environment presents a constant demand to detect evolving threats while promoting a positive passenger experience. The end goal is to reach non-invasive security screening at our nation's airports while meeting its mission of preventing terrorist attacks and ensuring speedy and lawful trade and travel. The aviation needs of the department focus around detection of threats on passengers and in baggage, in addition to authenticating the identity of passengers.

- As passengers receive a Transportation Security Administration (TSA)-defined passenger clearance ranking, it would be advantageous to link the ranking to a passenger's checked baggage to assist operators in the baggage screening process.
- Passengers can present a variety of forms of identification to Transportation Security Officers for security screening at the airport. The ability to quickly and accurately identify and verify these multiple types of identification is a key part of aviation security. Improved capabilities to verify a passenger's identity against the provided identification would help to expedite this process.
- Screening of passengers for threats concealed under clothing allows Transportation Security Dfficers to identify and mitigate threats to aviation security. DHS seeks an enhanced capability to conduct primary screening of passengers at aviation security checkpoints that results in reduced divestiture and expedited screening.
- TSA has shifted to a risk-based, intelligence-driven security model. TSA looks to improve capabilities to support operator decision making in passenger and carry-on baggage screening and enhance the ability to adjust security posture based on risk.
- Security threats are constantly evolving and present new challenges in screening passengers and baggage. DHS is looking to improve its efficiency in screening passengers' carry-on and checked baggage for prohibited items.
- Cargo security threats continue to evolve, making it necessary for DHS to identify enhanced screening methods against cargo threats.

Biological Threat: Biological threat security focuses around the prevention of release as well as detection of and protection against priority biological threats and hazards known to pose particularly high risk to the nation. Operators related to this threat area play a variety of roles and require personal protective equipment, detection and warning tools, and modeling and predictive analytics capabilities.

- In the event DHS operators are exposed to a biological threat, improvements in current escape hood personal protective equipment (PPE) will be beneficial. The PPE must be compact, portable, and quickly deployable while providing a full spectrum of protection.

- In the event of a biological attack or release, knowing what to do next is key and requires improved decision support tools. Improved decision support systems that integrate planning assumptions, formulas, and algorithms into one tool are required to translate situational awareness and intelligence into guidance to inform decision making. This also includes the use of PPE.
- For a wide range of DHS field agents, identifying a biological agent is critical to the overall response. The Department is interested in identifying improved means for field agents to detect, identify, and classify the presence of specific agents in a variety of settings. The overall process must be cost-effective and must not impede operations.
- The way a biological agent behaves once released is a major factor in responding to an event. Dispersion event modeling is needed across various media and environments for a wide array of biological agents, as well as human and animal diseases that are transmissible via air, water, and non-organic hosts. The modeling must include the transport of biological agents within the soil, surface, and atmosphere continuum, and provide numerical estimates and graphical analysis of their dispersion.
- It is essential that the Department expand its data assimilation and predictive analysis to inform decision making in the field and operations centers. This includes assimilation and analysis of situational awareness, models, planning assumptions, and surveillance data in a manner that provides real-time trend analysis and intelligence to predict operational risks and capability requirements. The capability must include a scalable, mathematical algorithm that estimates risks for individual trade and travel entities and provides: 1) "pattern of concern" recognition; 2) associations between entities from various port of entry environments (e.g., cargo, passenger, express consignments, international mail); and 3) alerting capabilities.
- The Department is seeking advancements in its ability to quickly verify biological attacks or releases by improving technologies and processes from the point of sampling and detection to testing. This capability should include the ability to obtain immediate confirmation of a biological incident that will allow for improved protective measures and deployments.

Border Security: DHS is responsible for securing our borders while expediting lawful trade and travel. This includes the security of 7,000 miles of terrestrial border with Mexico and Canada, air domain awareness within the United States, the security of the maritime approaches of the United States, and security of the nation's air, land and sea ports of entry. Border security presents complex challenges due to geographic locations, modes of transportation, trade and travel volume, and transnational criminal organizations.

- The Department is seeking to strengthen security and increase efficiency of DHS Traveler Inspection Operations at entry to and exit from the country by more effectively using information, new technologies, and process optimization to recognize dangerous individuals and facilitate rapidly growing lawful travel, trade, and tourism. Advancements in biometric and identity technologies, mobile capabilities, and other complementary capabilities will enable access to real-time information, increase situational awareness, and enable holistic improvements for travelers and DHS officers as well as airport, airline, and other stakeholders. The capabilities must be suitable for use by a demographically diverse traveler population, cost-effective, simple, transparent, and able to integrate seamlessly into the inspection/travel process.

- Non-intrusive inspection technologies allow DHS border agents and officers to detect contraband and illegal activity at air, land, and sea ports of entry while expediting lawful trade and travel. The Department is looking to increase the performance of existing inspection systems while also developing new non-intrusive inspection capabilities.
- Criminal organizations fly small aircraft at low altitudes across U.S. borders and within the U.S. to transport illegal drugs and support other illegal activity. The Department is looking to expand its ability to detect these aircraft and enable their timely interdiction. This ability must provide reliable and accurate detection, tracking, and classification of small, low-flying aircraft, including unmanned aircraft systems (UAS) and non-traditional aviation technologies (NTAT), such as ultralights or gyrocopters. Additionally, once a UAS/NTAT has been captured, law enforcement needs the ability to perform forensics to aid in the investigation and prosecution of any criminal activity.
- DHS is looking to increase the Department's sensor and intelligence information-sharing and data analytics capability. The goals include: 1) providing the ability to collect, identify, prioritize, characterize, and integrate existing maritime, land, air, and port of entry data from Federal, State, local, tribal, and international sources; 2) performing data analytics to turn the data into actionable intelligence; and 3) sharing that actionable intelligence with Federal, State, local, tribal, and international law enforcement partners.
- Border security along the northern and southern terrestrial borders of the United States presents a host of challenges. DHS is seeking to expand its situational awareness of the land border in-between land ports of entry. Improvements should include proficiency in detecting, tracking, and classifying illegal smuggling or immigration activity in difficult terrain, during harsh weather, and in remote locations along the northern and southern borders.
- Cross-border tunnels are dug by transnational criminal organizations to smuggle contraband, people, and potentially weapons of mass destruction into and out of the United States. The Department is seeking to improve the detection of cross-border tunnels, exploit them after they are found, and perform forensics and other investigative actions required to identify the organizations and people responsible.
- Remote maritime smuggling routes present challenges for DHS law enforcement. The Department is looking to advance its maritime surveillance and communications capability for remote, off-shore, illegal smuggling routes and U.S. statutory areas of responsibility, including the Atlantic, Pacific, Gulf of Mexico, Great Lakes, and Arctic regions. This includes improving shore-based sensors and exploiting offshore detection capabilities to increase DHS's maritime situational awareness.
- Small vessels can go undetected by law enforcement and be used to smuggle people or contraband, perform reconnaissance, or convey weapons of mass destruction. The Department is seeking enhancements to its small vessel detection capabilities to reliably and accurately detect, track, and classify small vessel threats (including pangas, semi-submersibles, go-fast boats, and other vessels) to enable their timely interdiction.

Cybersecurity: Cyber-threats could have detrimental impacts to the nation's economy and security. Integrated into our nation's critical infrastructure across the government and the private sector, cybersecurity is a top concern for DHS. The growth of the Internet of Things, cyber criminals, and a growing dependence on digital devices bring layers of complexity to cybersecurity that require technological advances.

- To ensure the security of cloud-based solutions, it is essential to have the capability to identify malicious and/or anomalous behavior and quickly mitigate the potential damage that behavior could cause. The Department is seeking to increase and improve distributed cloud-based communications and monitoring agents for identifying the malicious behavior of other entities within a distributed system. In addition, DHS would like an expanded ability to characterize the limitations of actionable analysis of different levels of administrative access; develop algorithms capable of operating at different privilege levels; and provide the capability to identify and characterize threat vectors specific to use and communicate with cloud-based computational clusters and storage.
- Securing industrial control systems that enable the operation of the nation's critical infrastructure is an essential element of our nation's security. DHS is looking for more robust sensor data collection, analysis, and prevention capabilities for industrial control systems and their associated systems.
- To solve cases, forensic examiners increasingly rely on the data stored on a variety of digital devices. To expand its support for law enforcement operators, DHS is looking to improve existing or develop new methods to extract and analyze data from networked devices (the "Internet of Things") for examination and use as evidence in criminal cases.
- Understanding the effectiveness of cybersecurity efforts is essential to any successful cybersecurity program. The Department is looking for improved methods to measure cybersecurity effectiveness, including the ability to measure incident severity and to compare security metrics. DHS is seeking methodologies that can compare security metrics (algorithms, efficiency, completeness, and correctness) such that disparate metrics can be combined to improve security situational awareness and help inform future capability deployment and funding decisions.

R&D Efforts to Develop Technology Solutions

The FY16 IPT process also identified existing R&D efforts that address the highest-priority technological capability gaps. DHS R&D efforts were identified in two ways. The sub-IPTs and IPTs documented R&D projects as they worked to identify priority capability gaps within their mission areas. In addition, S&T initiated a data call to all DHS components requesting information on ongoing research and/or development activities. The information compiled through these efforts represents the *Report of Coordinated DHS R&D*.

The IPTs then identified R&D efforts that address high-priority gaps. For gaps with insufficient or no corresponding R&D, the SRC recommended additional or new R&D investments to address those gaps. The specific additional or new R&D will be addressed through various S&T and component resource allocation processes and is expected to influence the Resource Allocation Plan for FY18 and beyond. The SRC-identified high-priority technological capability gaps and the existing R&D efforts that address those gaps are presented in the *High-Priority Technology Solutions* document.

Resilience as a Factor in Priority Ranking

Resilience continues to evolve as a factor influencing R&D efforts across multiple DHS missions. Resilience is defined as *the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.*[1] The IPTs identified technological capability gaps and ranked them as high, medium, or low priority within their specified mission areas. As the IPT process evolves, the priority ranking methodology will incorporate an ability to evaluate gaps and related R&D efforts based on the extent to which they enhance resilience at a national, community, or individual asset level.

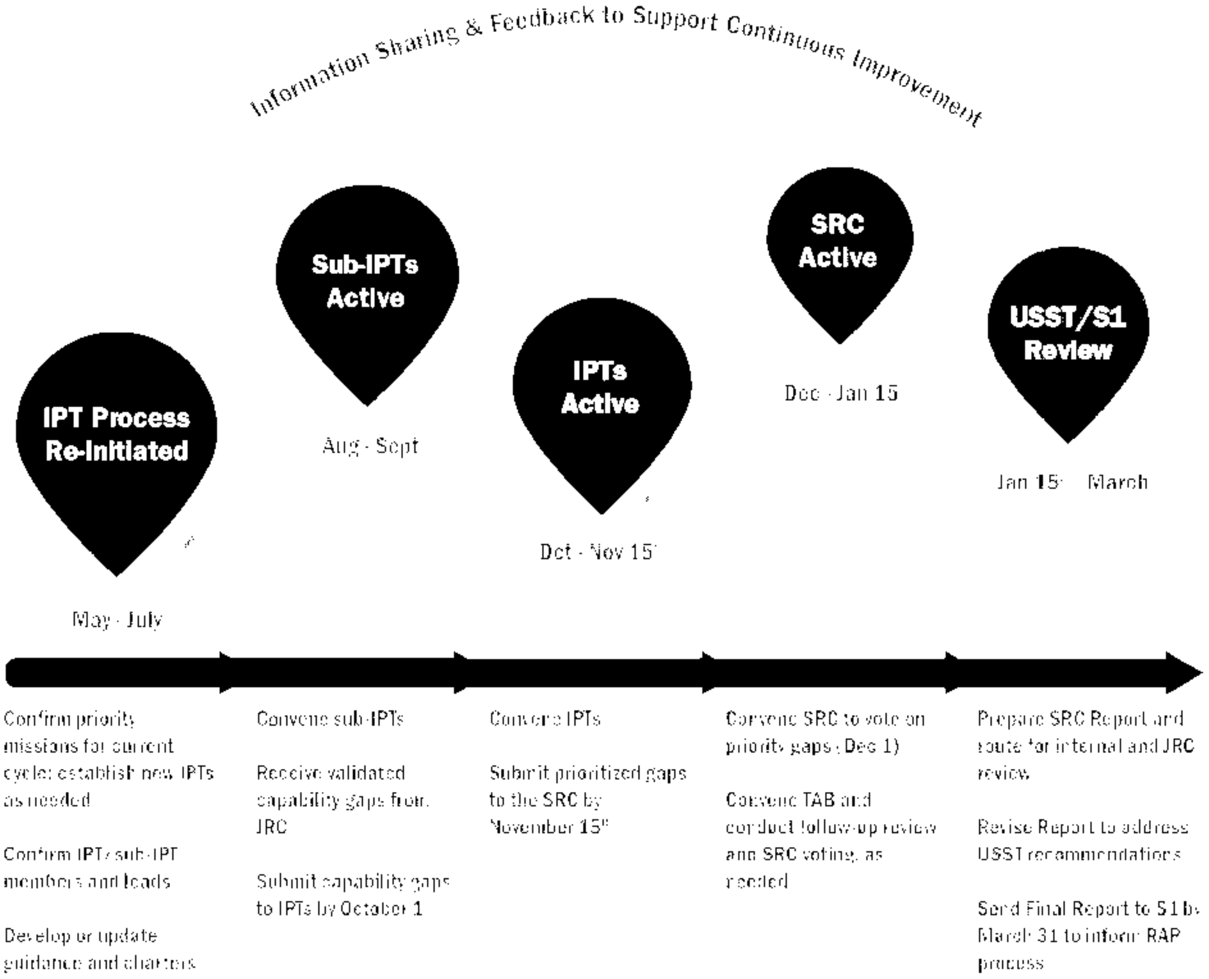
During the FY16 IPT cycle, DHS conducted an additional analysis focused specifically on identifying resilience-oriented efforts. Each of the described gaps and corresponding R&D efforts was evaluated for its contributions toward building resilience. An initial set of weighted resilience indicators aided in the process of identifying and classifying these efforts. This analysis lays the groundwork for linking resilience considerations to the priority ranking of gaps in future IPT cycles.

[1] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, February 2013.

V. Implementation: A Department-wide Approach

The IPT Process in Future Years

The IPT process outlined in this report proved effective in producing results in FY16, despite the abbreviated timeline and the effort required in establishing the IPTs. Consistent with the Secretary's guidance, the process must be repeatable and flexible to provide a robust foundation for current IPT operations and future evolution of the process. Figure 3 illustrates how the IPT process will continue as an annual cycle.



Confirm priority missions for current cycle; establish new IPTs as needed

Confirm IPT/sub-IPT members and leads

Develop or update guidance and charters

Convene sub-IPTs

Receive validated capability gaps from JRC

Submit capability gaps to IPTs by October 1

Convene IPTs

Submit prioritized gaps to the SRC by November 15th

Convene SRC to vote on priority gaps (Dec 1)

Convene TAB and conduct follow-up review and SRC voting, as needed

Prepare SRC Report and route for internal and JRC review

Revise Report to address USST recommendations

Send Final Report to S1 by March 31 to inform RAP process

Figure 3. IPT Annual Process and Timeline

It is important to note that the timeline depicted here reflects only the sub-IPT and IPT efforts that focus on developing final lists of high-priority gaps for consideration and ranking by the SRC for a given fiscal year. The IPTs and sub-IPTs are free to meet throughout the year, as they deem necessary, to collaborate on identifying and consolidating high-priority technological capability gaps within their mission areas.

The DHS enterprise continues to strive toward institutionalizing a systematic, component-driven approach that leverages a well understood and accepted definition of R&D to provide consistent outcomes in successive years.

The DHS IPT process is designed to:

- Identify duplicative DHS R&D activities and recommend ways to reduce duplication;
- Provide an oversight platform to coordinate cross-component collaboration and track the investment profile of each project to ensure progress and schedule maintenance; and
- Result in the development and transition of effective solutions to address priority technological capability gaps across the Department.

Because the priority ranking of gaps may lead to R&D investment decisions involving multiple components, it is critical that the process for determining priorities be credible, transparent, and as objective as possible. This will help to instill confidence among component and external stakeholders that DHS is identifying and addressing critical homeland security research needs.

Ensuring Continuous Improvement through Future Cycles

IPTs are used effectively across the Federal Government to bring together diverse stakeholders to work collaboratively toward a common goal. Despite the success of many well executed IPTs, the IPT approach is often poorly understood, defined, designed, and implemented. The DHS IPT process includes a series of steps to ensure the identification, prioritization, and coordination of all R&D within the Department. These steps include:

- Defining clear objectives and outcomes for the IPTs;
- Developing a common process and approach for the IPTs;
- Establishing a governance structure that allows for growth and improvement while maintaining foundational guidance and metrics to achieve targeted outcomes;
- Executing IPT activities, which requires gaining component consensus while maintaining IPT process integrity; and
- Providing ongoing management and evaluation to ensure that the process remains effective over the long term.

The last step above is the most critical to the sustainability of the DHS IPT process. The IPTs and S&T representatives will document lessons learned throughout the process. Because evaluation of the IPT process should not rest with one entity, S&T initiated an annual, independent After Action Review (AAR) of the IPT process. The AAR will provide an objective assessment of the process and validate linkages to the priorities of DHS components, to demonstrate credibility with internal and external stakeholders.

The AAR will provide recommendations for ensuring a sustainable, defensible IPT process for future years by:

- Evaluating the priority ranking methodology and any metrics used to assess component needs, for validity and transparency;

- Evaluating the results of each IPT cycle, to assess whether it produced a reasonable set of high-priority gaps and corresponding R&D efforts (investments); and
- Identifying lessons learned and providing recommendations for corrective actions and process improvements that can be implemented in future IPT cycles.

Alignment of the IPT and JRC Processes

The IPTs and the JRC follow two distinct but mutually supportive and interdependent processes. The IPTs focus on R&D efforts while the JRC focuses on operational requirements, but there are several touch points that present important information-sharing opportunities for the IPTs and JRC. Figure 4 on the next page illustrates the touch points between the two processes.

Through the Joint Requirements Integration and Management System (JRIMS) process, the JRC reviews and validates component-submitted operational capability gaps, associated requirements, and proposed courses of action to mitigate those gaps.

As noted earlier in this report, during the FY16 cycle, JRC representatives participated in the sub-IPTs and had a voting seat on the SRC to provide expertise in requirements and gap identification and facilitate information sharing between the two processes.

By sharing information, the IPTs and JRC can leverage one another's expertise and reduce the reporting burden on DHS components. As the JRC builds out processes for operational capability gap collection and requirements validation and prioritization, resulting information outputs can be shared with the IPTs. Similarly, the IPTs can inform the JRC of capability gaps that may require R&D.

R&D efforts identified by the IPTs may develop solutions that are transitioned to component users through acquisition programs or used to fill a JRC-identified operational capability gap. In future cycles, the IPTs will continue to share information on current and planned R&D efforts and inform the JRC of technologies that are approaching transition readiness.

The JRC continues to mature its processes for joint assessment of requirements and operational capability gap prioritization. The level of direct interaction between the IPT and JRC processes will increase over time as the JRC assumes a lead role in prioritizing joint operational capability gaps and requirements. Future iterations of the IPT process will leverage existing analysis from other organizations in DHS to enhance the translation of JRC-identified operational capability gaps to IPT-identified technological capability gaps.

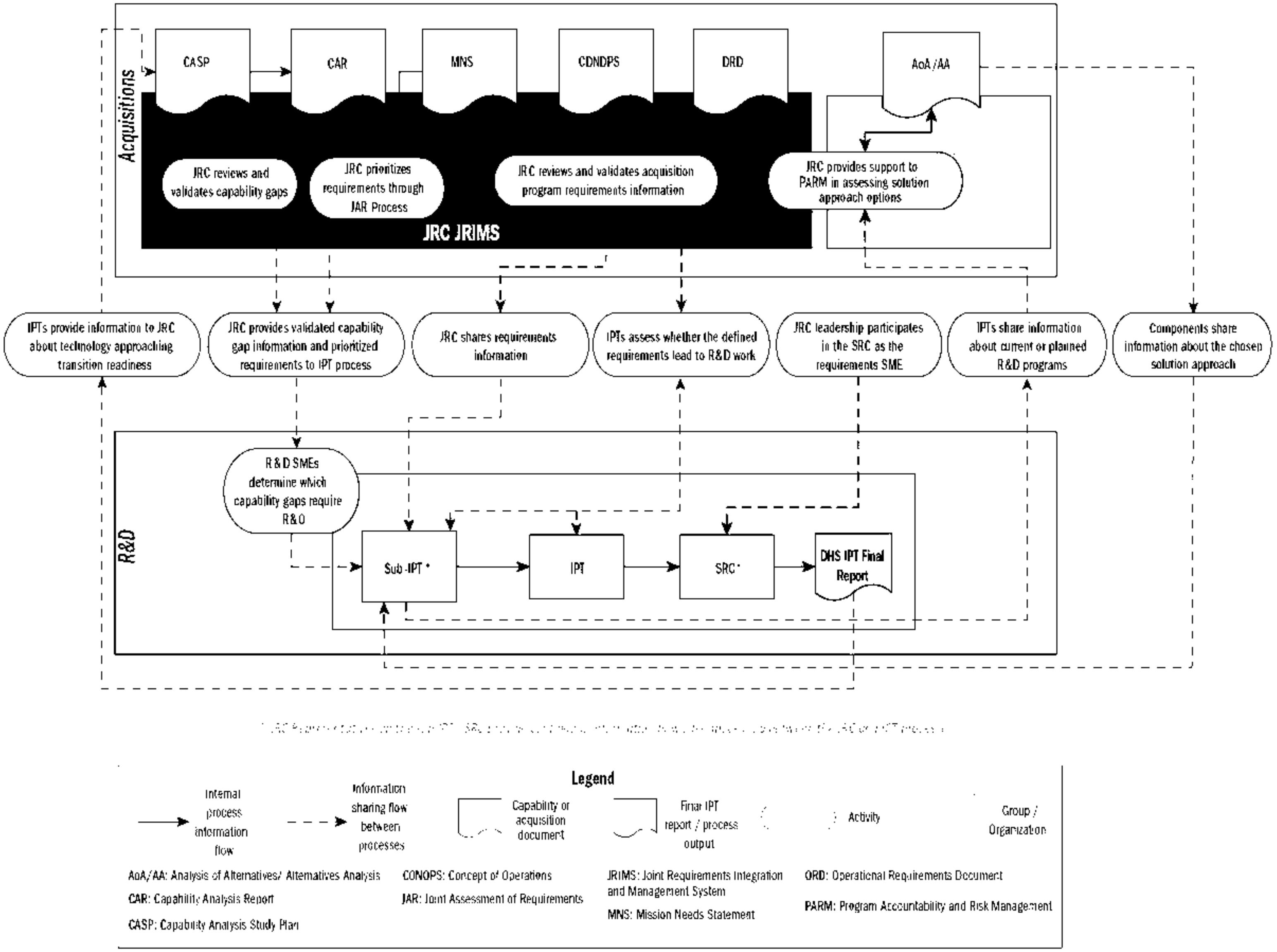

Acquisitions
CASP
CAR
MNS
CONOPS
ORD
AoA/AA
JRC reviews and validates capability gaps
JRC prioritizes requirements through JAR Process
JRC reviews and validates acquisition program requirements information
JRC provides support to PARM in assessing solution approach options
JRC JRIMS
IPTs provide information to JRC about technology approaching transition readiness
JRC provides validated capability gap information and prioritized requirements to IPT process
JRC shares requirements information
IPTs assess whether the defined requirements lead to R&D work
JRC leadership participates in the SRC as the requirements SME
IPTs share information about current or planned R&D programs
Components share information about the chosen solution approach
R&D
R&D SMEs determine which capability gaps require R&D
Sub-IPT *
IPT
SRC *
DHS IPT Final Report
[illegible]
Legend
Internal process information flow
Information sharing flow between processes
Capability or acquisition document
Final IPT report / process output
Activity
Group / Organization
AoA/AA: Analysis of Alternatives/ Alternatives Analysis
CAR: Capability Analysis Report
CASP: Capability Analysis Study Plan
CONOPS: Concept of Operations
JAR: Joint Assessment of Requirements
JRIMS: Joint Requirements Integration and Management System
MNS: Mission Needs Statement
ORD: Operational Requirements Document
PARM: Program Accountability and Risk Management

Figure 4. Alignment of IPT and JRC Processes

Development and Transition of Solutions to Address Priority Gaps

The Secretary charged the IPTs with developing and reporting metrics for the transition of technological solutions to close capability gaps. To support this objective, DHS developed a process (see Figure 5) for assessing high-priority gaps to inform decisions on solution development and transition. Each step in the process requires coordination among the three appropriated R&D entities within DHS (DNDO, USCG, and S&T) and other DHS components with equities in a given gap.

The first step ensures an understanding of the mission need associated with a priority gap to support further analysis. During the second step, analysts identify existing technology opportunities and market information that may support a gap.

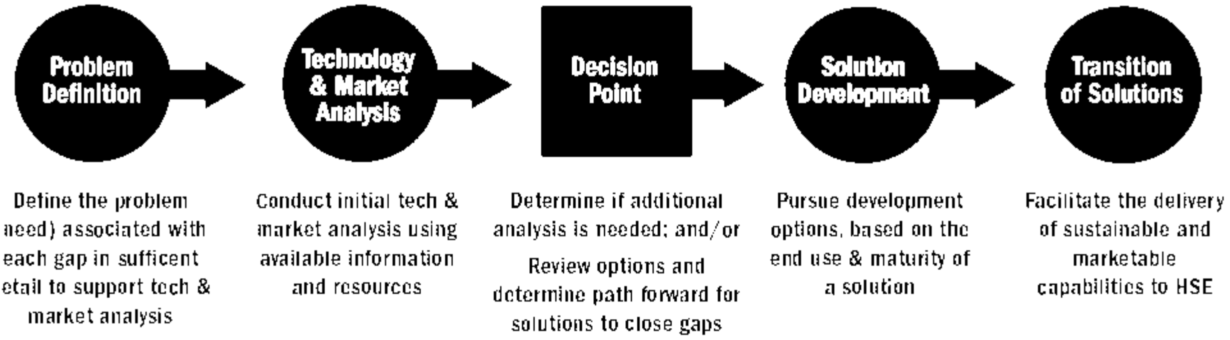

Problem Definition
Technology & Market Analysis
Decision Point
Solution Development
Transition of Solutions
Define the problem (need) associated with each gap in sufficent detail to support tech & market analysis
Conduct initial tech & market analysis using available information and resources
Determine if additional analysis is needed; and/or
Review options and determine path forward for solutions to close gaps
Pursue development options, based on the end use & maturity of a solution
Facilitate the delivery of sustainable and marketable capabilities to HSE

Figure 5. Assessing High-Priority Gaps to Support Solution Development and Transition

A decision point occurs between the second and third steps in the process, when sufficient information exists to support decisions on solution development or refinement. If sufficient information does not exist, a decision can be made to perform additional analysis. Based on initial findings, component and S&T representatives will coordinate with other DHS and external partners to review options and support an appropriate path forward to close priority gaps. Transition planning is an integral consideration throughout the process to ensure the proposed solution can and will be appropriately transitioned for use.

Appendix B provides more information on developing and transitioning solutions to address high-priority gaps.

Technology Assessments and Acquisition Programs

In the August 2015 memo, the Secretary directed S&T to conduct a systems engineering review and technology assessment of the technical solutions in major DHS acquisition programs and provide a report to the Chief Acquisition Officer and the JRC prior to the decision to enter the "obtain" phase of the Acquisition Life Cycle. The results of the IPT process can inform a DHS acquisition profile that aligns to the high-priority technological capability gaps across DHS mission areas. Technology assessments help to ensure the technical readiness and feasibility of solutions intended to address those high-priority gaps.

S&T has begun to conduct technical assessments on proposed and established Department acquisition programs. A technical assessment is a combined system engineering review of an acquisition program and an assessment of the technologies that are necessary to realize the capability that the acquisition program intends to deliver. S&T will conduct technical assessments of ongoing acquisition programs in FY16 and will conduct additional assessments in FY17 and beyond. In the future, where an assessment determines that major technical risk and/or overall program risk is high, follow-on technical assessments may be conducted during the acquisition cycle to monitor these risks.

Systems engineering technical assessments provide greater understanding of the technical maturity of solutions that DHS intends to acquire. The results of these assessments provide information on:

- The ability of an acquisition program to deliver the needed capability on schedule;
- Potential opportunities to augment the program with new or additional capabilities; and
- Potential new gaps and associated R&D efforts that could be addressed through proposed and existing acquisition programs.

VI. The IPTs in Summary: Current and Next Generation

In August 2015, the Secretary issued a memorandum directing the establishment of IPTs to identify DHS technological capability gaps and coordinate R&D efforts to close those gaps across the mission areas of the Department. Consistent with the Secretary's guidance, S&T developed an initial IPT process that delivered results in FY16 and provides a solid blueprint for future evolution. The initial IPT level of effort established an IPT governance structure, guidance, data collection templates, and an outreach platform available across the Department. DHS components implemented the process through three main bodies–sub-IPTs, IPTs, and the SRC–and incorporated feedback from additional DHS HQ organizations through the Technical Advisory Board (TAB). The process supports Departmental unity of effort by facilitating cross-component collaboration and traceability of R&D efforts.

The Secretary outlined the following primary objectives for the IPTs:

- Identify and prioritize technological capability gaps and corresponding efforts to develop solutions to close those gaps;
- Identify R&D being performed across DHS, both in traditional R&D funding lines and in component acquisition programs;
- Ensure that technology being acquired meets DHS and component mission needs;
- Identify and de-conflict duplicative R&D efforts; and
- Develop and report metrics for the transition of technological solutions to close gaps.

The two documents delivered to the Secretary address the first two objectives. The IPT process established for the FY16 cycle provides the foundation to achieve the remaining three objectives in future cycles. In so doing, the IPT process will address the GAO recommendations to improve R&D tracking and coordination across the Department.

S&T established five chartered IPTs in FY16, all of which had active sub-IPTs that met and identified mission-focused capability gaps. Four of the five IPTs completed the process by providing priority gaps to the SRC.

During the FY16 IPT process, DHS conducted an additional analysis focused specifically on identifying cross-cutting, resilience-oriented efforts. Because resilience influences R&D activities across multiple mission areas, DHS evaluated the IPT-identified priority gaps and corresponding R&D efforts for their contributions toward enhancing resilience.

Building on the process established to date, the IPTs will continue to evolve as the central mechanism by which the Department identifies and coordinates its R&D efforts to DHS priority missions. To ensure a sustainable and defensible process for future years, S&T initiated an annual, independent AAR of the IPT process. The initial AAR will assess the effectiveness and transparency of the methodology and results from the FY16 process and identify lessons learned to support recommendations for improvement in future cycles.

Acronym List

AAR	After Action Review
CBP	U.S. Customs and Border Protection
CIO	DHS Chief Information Officer
CRCL	DHS Office of Civil Rights and Civil Liberties
CT	Counterterrorism
DHS	U.S. Department of Homeland Security
DNDO	DHS Domestic Nuclear Detection Office
FEMA	Federal Emergency Management Agency
FRRG	First Responder Resource Group
FY	Fiscal Year
GAO	Government Accountability Office
HSE	Homeland Security Enterprise
I&A	DHS Office of Intelligence and Analysis
ICE	U.S. Immigration and Customs Enforcement
IED	Improvised Explosive Device
IPT	Integrated Product Team
JRC	DHS Joint Requirements Council
JRIMS	Joint Requirements Integration and Management System
MGMT	DHS Directorate for Management
NPPD	DHS National Protection and Programs Directorate
OHA	DHS Office of Health Affairs
PLCY	DHS Office of Policy
PPE	Personal Protective Equipment
R&D	Research and Development
S1	Secretary of Homeland Security
S2	Deputy Secretary of Homeland Security
S&T	DHS Science and Technology Directorate
SRC	Science and Technology Research Council
TAB	Technical Advisory Board
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	U.S. Secret Service
USST	Under Secretary for Science and Technology

Appendices

This section contains appendices that provide supporting information on topics referenced in the report, as follows:

- **Appendix A: Integrated Product Team Structure and Functions** – Describes the IPT governance structure and functional process established in FY16.
- **Appendix B: Development and Transition of Solutions to Address Priority Gaps** – Outlines the process by which DHS will assess high-priority gaps to support decisions to develop and transition solutions to address those gaps; and describes DHS activities that support solution development and transition.

Appendix A - Integrated Product Team Structure and Functions

In response to the Secretary's August 2015 memorandum, S&T established an operational framework and process for FY16 to support the stand-up, governance, and ongoing operations of the IPTs. Composed of three main implementing bodies—sub-IPTs, IPTs, and the S&T Research Council (SRC)—plus an advisory board, the FY16 IPT process engaged executives and staff from across DHS to identify technological capability gaps and priority R&D efforts to close those gaps.

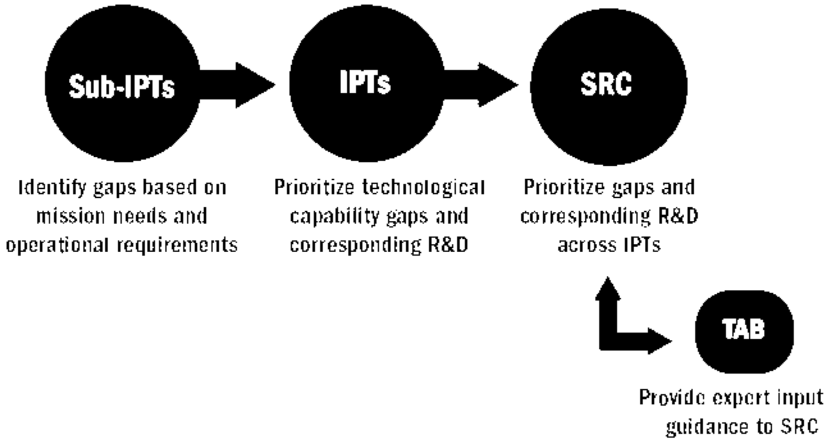

Sub-IPTs
IPTs
SRC
Identify gaps based on mission needs and operational requirements
Prioritize technological capability gaps and corresponding R&D
Prioritize gaps and corresponding R&D across IPTs
TAB
Provide expert input & guidance to SRC

Figure 1. IPT Governance Structure

Sub-IPTs

The sub-IPTs included component and S&T staff with expertise in a specified topic within the larger mission area of their respective IPT.

The bulk of work performed as part of the IPT process was accomplished at the sub-IPT level. A representative from the JRC participated on each sub-IPT to ensure alignment with the JRC process and consideration of the requirements identified through that process. In FY16, the sub-IPTs performed some or all of the following activities:

- Identifying high-priority technological capability gaps based on mission needs and operational requirements;
- Documenting ongoing DHS R&D activities within their area of focus; and
- Identifying R&D efforts that address high-priority gaps.

Integrated Product Teams

The IPTs were composed of senior-level staff and executives from across DHS who are empowered to act on behalf of their components. IPT members worked collaboratively to conduct some or all of the following activities in FY16:

- Considering the technological capability gaps identified by the sub-IPTs and developing a list of high-priority gaps across the IPT mission space;
- Validating any ongoing DHS R&D activities identified by the sub-IPTs; and

- Reviewing R&D activities identified by the sub-IPTs and generating a list of R&D efforts that address high-priority gaps across the mission space.

In addition to inputs from the sub-IPTs, the IPTs considered additional component needs that fell within the scope of the IPT mission, as well as any new or emerging priorities identified by Department leadership or dictated by real-world events.

The IPTs worked closely with legal, policy, civil liberties, and privacy advisors to ensure that appropriate protections were built into planned outcomes and issues were addressed through review and adjudication cycles.

S&T Research Council

For FY16, the SRC included the component senior executives who chair the IPTs, a chair from S&T, and a senior representative of the JRC. Each IPT provided the SRC with a list of high-priority mission-focused gaps and corresponding R&D efforts. The SRC reviewed the consolidated inputs from the IPTs and generated a list of high-priority technological capability gaps and corresponding R&D efforts across the IPTs.

A senior representative of the FRRG also participated in the SRC, to ensure alignment and awareness of top-priority needs of responders in the field. The FRRG identified priority capability gaps and R&D efforts for the State and local responder community and submitted this information to the SRC. The FRRG provided input to SRC deliberations as appropriate, but did not vote on the DHS component-driven priorities identified by the IPTs.

To ensure a broad view across the full spectrum of DHS R&D, the SRC required input from many stakeholders within DHS, beyond the information provided by the IPTs. This report reflects that additional input, gleaned primarily from two sources:

1) A data call to all DHS components to identify ongoing research and/or development activities across the Department; and

2) A Technical Advisory Board (TAB) that reviewed and advised on SRC recommendations and draft products.

Technical Advisory Board

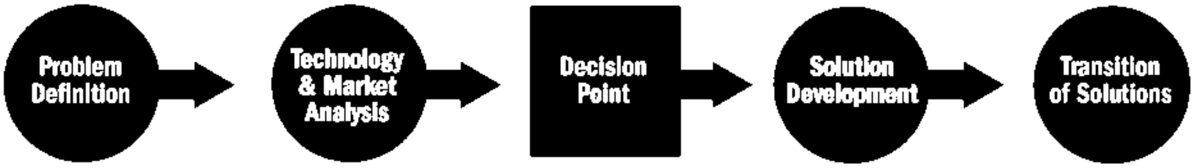
The TAB included senior representatives from DHS HQ components and offices that did not participate in the IPTs. Chaired by the DHS Office of Policy, the TAB provided advice on key milestones and recommendations, as requested by the SRC.

In FY16 and going forward, the TAB may conduct or support the following activities:

- Reviewing and commenting on draft SRC products;
- Responding to queries related to the technical content or execution of the IPT process;
- Providing input to a consensus-based process for ranking gaps and corresponding DHS R&D activities in accordance with SRC guidance.

Appendix B - Development and Transition of Solutions To Address Priority Gaps

The Secretary identified several objectives for the IPT process, including developing and reporting metrics for the transition of technological solutions to close capability gaps. To this end, DHS developed a process to assess the high-priority gaps identified by the SRC to inform decisions on how best to move forward in addressing the gaps. This process, illustrated in the figure below, requires coordination across DHS to ensure that all component equities are represented and that appropriate programs are leveraged to support process objectives.



Define the problem (need) associated with each gap in sufficent detail to support tech & market analysis

Conduct initial tech & market analysis using available information and resources

Determine if additional analysis is needed; and/or

Review options and determine path forward for solutions to close gaps

Pursue development options, based on the end use & maturity of a solution

Facilitate the delivery of sustainable and marketable capabilities to HSE

Figure 1. Assessing Priority Gaps to Support Solution Development and Transition

The first step ensures an understanding of the mission need associated with a priority gap to support further analysis. Analysts then identify existing technology opportunities and market information that may support a gap. A decision point occurs between the 2nd and 3rd steps, when sufficient information exists to support decisions on solution development or refinement. If more information is needed, additional analysis may be pursued.

To implement the process effectively, a dedicated team will be formed to focus on each gap. These teams should include component and S&T program managers and other subject matter experts with working knowledge of the gap, as well as representatives of DHS activities that support the development and transition of solutions to address the gap. The technology scouting and technology transition activities play a role throughout the process, as described below.

Technology Scouting and Market Analysis

Technology scouting and market analysis provide critical information about technologies that are or have been developed, deployed, and utilized in a given market sector. This information enables DHS to make better decisions about how it invests in R&D. This information can:

- Identify existing technologies that could be adopted or modified;
- Determine what technologies are being used and/or acquired in a given market;
- Provide information on legacy systems, buying patterns, lifecycle and maintenance costs, and regulatory and policy issues; and
- Isolate early adopters of new technologies.

Technology Transition

DHS provides mechanisms and services that support the conversion of technologies, standards, and knowledge products to the operational environment. This process includes leveraging the technology scouting and market analysis activities described above; designing formal transfer agreements, employing tools such as Partnership Intermediary Agreements (PIA) and Cooperative R&D Agreements (CRADA); assisting with patent applications; and tracking and managing intellectual property for DHS and its partners.

Brief descriptions of other programs and activities that support solution development and transition are presented below, in alphabetical order.

Center of Innovation. S&T manages the United States Air Force Academy (USAFA) Center of Innovation (CoI), which is designed to create novel capabilities from emerging industry research technologies that will eventually enable commercial off-the-shelf (COTS) products. The CoI enables the Federal Government to conduct cooperative research with leading private industry technology companies. The CoI is in the process of integrating several industry technologies to examine alternatives for better communication and collaboration among Federal Government organizations.

In-Q-Tel. In-Q-Tel (IQT) is an independent, not-for-profit organization that invests in venture capital startup companies that support intelligence and homeland security needs. IQT provides a conduit through which DHS can anticipate and leverage technology trends to support near-term development and piloting activities that address prioritized capability gaps.

Interagency Programs. DHS develops trusted partnerships with other Federal Government agencies to leverage combined investments and resources in support of R&D programs and initiatives. The Homeland Security Act of 2002 gives S&T the responsibility to coordinate with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs.

International Programs. DHS develops partnerships with foreign governments and international organizations to enhance scientific and technical knowledge for the homeland security enterprise (HSE). These partnerships will provide HSE stakeholders with access to innovative R&D knowledge, funding, and other unique capabilities and resources. S&T currently manages partnerships with Australia, Canada, France, Germany, Israel, Mexico, the Netherlands, New Zealand, Singapore, Spain, Sweden, the United Kingdom, and the European Commission.

National Laboratories. DHS maintains critical laboratory assets and coordinates related activities to support technological innovations, scientific breakthroughs, rapid response capabilities, and solution deployment. S&T oversees a network of five DHS laboratories and coordinates with 13 Department of Energy (DOE) National Laboratories in support of DHS priorities and missions. The DOE Labs can support the gap assessment process by helping to validate capability gap analyses and improve requirements generation.

Operational Experimentation. Operational Experimentation (OpEx) is a method of operational analysis designed to generate end-user feedback on operational requirements and technologies to support a broad range of homeland security stakeholders. This process demonstrates technologies in real-world scenarios to determine operational constraints and the efficacy of a sponsored technology in a given mission space. Ideally, there will be

OpEx events centered on specific capability gaps identified by each of the IPTs. The results of these events will be coordinated with the Joint Requirements Council to inform DHS acquisitions that address priority needs.

PIONEER. The goal of the Partnering for Innovation and Operational Needs through Embedding for Effective Relationships (PIONEER) program is to develop better relationships and enhance interaction between S&T and DHS components to increase understanding of research and development processes. This program embeds S&T scientists into the operational environments of DHS components, enabling current-state awareness of the components' most critical needs. Concurrently, DHS component personnel are embedded into the S&T research, development, test, and evaluation processes.

Prize Competitions. DHS prize competitions engage a broad range of talent through public crowdsourcing to produce ideas and solve tough homeland security challenges. Prizes are most effective when there is a well-defined problem and the results of a competition can produce change. DHS announces a problem or question to the public (usually through publication in the Federal Register), along with specific criteria for evaluating entries. A diverse group of judges then assesses the submissions against stated criteria and ensures that desired results are achievable.

Research & Development Accelerators. The DHS Accelerator program is designed to attract innovators, while keeping pace with the speed of technological advancement. Accelerators provide DHS with visibility and allow for engagement with startup companies that are developing cutting-edge technologies. Accelerators and their private sector networks provide a cost-effective way to engage a multitude of high-quality companies and influence their development to align with DHS priority needs.

SAFETY Act Implementation. DHS has an office devoted to implementing the SAFETY Act, a law that may limit the legal liability of companies that manufacture or sell technologies and services that have anti-terrorism capabilities. The "Support Anti-Terrorism by Fostering Effective Technologies" (SAFETY) Act was enacted by Congress as a direct result of 9/11 and as part of the Homeland Security Act of 2002 (Title VII, Subtitle G). By capping liability, the law promotes the creation, deployment, and use of anti-terrorism technologies to protect the homeland and save lives.

Small Business Innovation Research (SBIR). The DHS SBIR Program provides early-stage funding, based on scientific merit, to U.S. small businesses to develop new technologies and innovations that have the potential to meet DHS R&D needs. DHS S&T's SBIR program is focused on near-term commercialization and delivery of operational prototypes to Federal, State, and local emergency responders and managers, as well as internal DHS entities. In addition, technology solutions resulting from SBIR funding provided by other Federal agencies can be leveraged through the S&T SBIR Program's Other Agency Technology Solutions (OATS) pilot program, helping to reduce the time from proof-of-concept feasibility to demonstration.

University Centers of Excellence. DHS manages 10 university Centers of Excellence (COE) that conduct research and education in support of DHS major mission areas. DHS components can use the COEs to answer research questions, access advanced capabilities and technical solutions, and find highly skilled future workers. COEs are broadly based in DHS mission areas and have the flexibility to address new problems or unexpected challenges, including those identified through the IPT process.

Research priorities for the COEs originate with the DHS components, which staff the Federal Coordinating Committees (FCCs) for each COE and select the most mission-relevant projects. The FCC process is focused on long-term challenges with uncertain outcomes, compared to the shorter term, better defined priorities addressed by the IPTs. Technological capability gaps prioritized through the IPT process will inform new research questions for the COEs. These questions will be considered annually and biennially in COE reviews, during which some research projects are discontinued and replaced by new ones.

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security

Project Responder 4

2014 National Technology Plan for Emergency Response to Catastrophic Incidents

July 2014

Homeland
Security

Science and Technology

TASK LEADS
Michelle Royal
David Jennings

TASK TEAM

Homeland Security Studies and Analysis Institute
Bryan Altmire
Elizabeth Dugan, Ph.D.
Kimberly Jones
Sherry Reichow, Ph.D.

Steve Chabolla

Manager, Business Enterprise Analysis Division

Daniel Kaniewski, Ph.D.

Director, Resilience Emergency Preparedness/Response Mission Area

PROJECT RESPONDER 4:

2014 National Technology Plan for Emergency Response to Catastrophic Incidents

July 2014

Prepared for
Department of Homeland Security
Science and Technology Directorate, Support to the
Homeland Security Enterprise and First Responders Group

For information about this publication or other research, contact:

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

Analytic Services Incorporated
5275 Leesburg Pike, Suite N-5000
Falls Church, Virginia 22041
Tel (703) 416-2000 • Fax (703) 379-2550
http://www.homelandsecurity.org/

Publication Number: RP13-17-02

TABLE OF CONTENTS

LIST OF FIGURES

(This page intentionally blank.)

EXECUTIVE SUMMARY

Project Responder 4 (PR4) is the fourth in a series of studies begun in 2003 to focus on identifying capability needs, shortfalls and priorities for catastrophic incident response. The approach for the PR4 study allowed a longitudinal look at 11 years of enduring gaps and needs, and distinguishing them from emerging needs and technology. The results of this study are captured in this *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents*.

PR4 identifies a set of enduring and emerging capability needs, frames them into technology objectives and assesses the state of science and technology to meet those needs. Findings are based on discussions with federal, state and local first responders as well as technical subject matter experts (SMEs). These interactions ensure that potential solutions reflect operational considerations and are based on an actionable and achievable technology path.

Capability Needs

This document identifies 14 capability needs that responders believe represent the highest priorities for improving their ability to respond to catastrophic incidents. Each of the capability needs may be improved, in whole or in part, through the application of technology solutions. The capability needs include enduring needs that were identified across the previous phases of Project Responder and emerging needs that will allow responders to leverage technological advances occurring in other fields. Responders prioritized these needs based on their impact on responder safety, population safety, consequence mitigation, decision-making and utility across multiple incidents.

Response Technology Objectives

This plan identifies 42 response technology objectives (RTOs) that address the 14 PR4 capability needs. The RTOs translate the capability statements into actionable, technology-centric objectives. Each identifies a high-level technology solution (or part of a solution) designed to improve the capabilities of the response community. Each capability need has at least one corresponding RTO, and some RTOs can address multiple needs. The RTO descriptions include projects that represent a proposed path forward for increasing capability. This plan also contains a series of technology road maps that illustrate the project timelines and resource requirements suggested by the SMEs for each RTO. In addition, the road maps highlight synergies and dependencies in the development process. This plan is intended to inform FRG as it makes investment decisions and proceeds with an acquisition strategy designed to address enduring and emerging emergency response needs. The capability needs and the related RTOs also provide DHS and other government agencies, academia and private industry with a vision toward which they can direct their efforts.

INTRODUCTION

Background

Responding to a large-scale catastrophic incident requires the coordination of personnel, equipment, communications, tactics, regulations and priorities, as well as the sharing of information and intelligence among many agencies and entities. This coordination and information sharing is difficult under normal circumstances but is exacerbated when the event is traumatic, the damage is widespread and the threats and dangers evolve. Inevitably, a catastrophic incident exceeds the resources of local jurisdictions, requires regional or national mutual aid and entails long-term response and recovery operations. There are gaps between what response agencies can currently do and what they feel is necessary for successful large-scale incident response. These gaps can be attributed to insufficient resources, procedures or training necessary to accomplish missions, or to changes that alter the response environment.

The Oklahoma City National Memorial Institute for the Prevention of Terrorism (MIPT) funded an effort in April 2001 to identify these gaps and improve the capabilities of local, state and federal emergency responders. That effort, called Project Responder, focused on identifying capability needs, shortfalls and priorities for catastrophic incident response. Because the response environment is constantly changing, Project Responder has periodically reevaluated capability needs by engaging emergency responders from a diverse set of disciplines and jurisdictions. Project Responder 4 (PR4) represents the latest iteration in this continuing effort.[1]

The purpose of Project Responder is to identify gaps between the current capability of emergency response agencies and what they consider necessary to respond to large-scale catastrophic incidents.[2] These gaps are prioritized and analyzed to produce actionable recommendations that have been used by DHS, other government agencies and private industry to guide development efforts that specifically address articulated operational needs. This effort is unique in its dedication to capturing the voices of responders from both traditional and nontraditional response agencies as they describe their needs and goals for policy, procedures and technology.[3]

It is beyond the ability of a single local or state agency to fund the development of new equipment, set universal standards for processes and procedures, facilitate the integration of existing resources and coordinate information-sharing protocols. State and local

[1] See Appendix A for a history of Project Responder.

[2] Catastrophic incidents are defined in this document to include large-scale natural disasters and man-made events (terroristic and accidental) that exceed the capabilities and resources of a local jurisdiction or region.

[3] Project Responder uses the terms "emergency responders" or "emergency response agencies" to be inclusive of traditional and nontraditional agencies that are necessary for response to catastrophic incidents. This includes public safety entities (i.e., law enforcement, fire, emergency medical services, emergency management) and supporting entities (e.g., public health, public works, transit).

budgets are tight, and threats and hazards are numerous. It is the mission of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) to provide support when capability gaps cannot be satisfied at the state and local levels and when investments in science and technology can provide advances to responders throughout the country. S&T has an office specifically designated for this purpose. The Support to the Homeland Security Enterprise and First Responders Group (FRG) strengthens the response community's abilities to protect the homeland and respond to disasters.[4] The FRG does this through the development of existing and emerging technologies, knowledge products and standards. To this end, FRG needs to understand the capability gaps and priorities of the emergency response community as well as the potential solutions to fill those gaps. This ensures that their investments are made efficiently and effectively.

Previous iterations of Project Responder identified the capability needs of emergency responders through multiple changes in the response environment over more than a decade. PR4 builds on these efforts by examining the state of science and technology for opportunities to address the most persistent and highest-priority capability needs and develops a plan to address those needs. The FRG tasked the Homeland Security Studies and Analysis Institute (HSSAI) to resume its efforts on Project Responder and to develop this plan.[5] This document, *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents,* identifies a set of enduring and emerging capability priorities, frames them into technology objectives and describes an incremental and actionable approach to technology development. This approach is illustrated through a series of technology road maps. Decision-makers, planners and acquisition personnel in the FRG are the intended audience for this document. However, the contents of this plan can also be used by other DHS and government agencies, academia and private industry to pursue targeted technology development opportunities.

This plan is based on an understanding of the capabilities needed to respond to catastrophic incidents. The technology programs identified as part of this plan correlate to the capability needs. HSSAI created this plan with the involvement and input of emergency responders, who have ultimate responsibility for response operations, and technical subject matter experts, who provided insight about the state of technology for these capabilities.

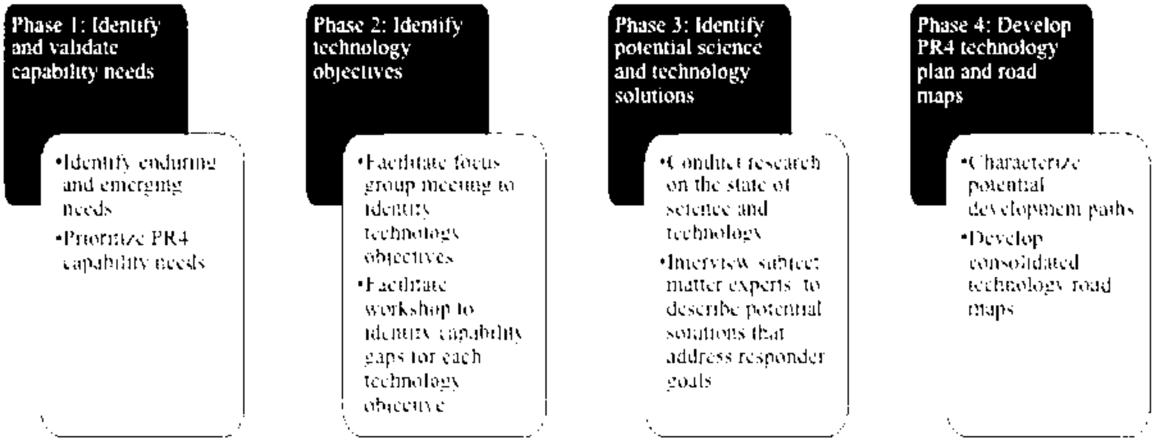
[4] "Science and Technology Directorate Support to the Homeland Security Enterprise and First Responders," U.S. Department of Homeland Security, last modification: n.d., http://www.dhs.gov/st-frg.

[5] In April 2004, the first Project Responder effort produced the *Project Responder National Technology Plan for Emergency Response to Catastrophic Terrorism* following an extensive effort to understand the capability needs of the emergency response community and identify potential solutions for those needs. The 2004 plan focused on technology investment to improve capabilities and included the development of technology road maps comprised of initiatives to close gaps in responder capabilities. This document is a second iteration of that document.

Methodology Overview

This section provides a brief overview of the analytical processes used to obtain and assess data and to develop the plan's findings. Appendix B provides a more detailed description of each phase in the methodology.

The methodology consisted of data gathering and analysis based on HSSAI's research and structured discussions with the response community and Subject matter experts. This occurred through four phases: (1) identification and validation of enduring and emerging capability needs; (2) identification of technology objectives to meet those needs; (3) identification of potential science and technology solutions; and (4) development of a technology plan and corresponding road maps. The graphic below illustrates this process:



Phase 1: Identify and validate capability needs

- Identify enduring and emerging needs
- Prioritize PR4 capability needs

Phase 2: Identify technology objectives

- Facilitate focus group meeting to identify technology objectives
- Facilitate workshop to identify capability gaps for each technology objective

Phase 3: Identify potential science and technology solutions

- Conduct research on the state of science and technology
- Interview subject matter experts to describe potential solutions that address responder goals

Phase 4: Develop PR4 technology plan and road maps

- Characterize potential development paths
- Develop consolidated technology road maps

Figure 1. PR4 Methodology

The goal of phase 1 was to identify the capability needs that should be addressed in the plan and to validate those needs with a group of emergency responders. To do so, HSSAI facilitated a series of virtual focus group meetings with members of the First Responders Resource Group (FRRG) and InterAgency Board (IAB).[6, 7] During the meetings, participants reviewed the capability priorities identified during Project Responder 3 (PR3) and suggested new or evolving needs. HSSAI identified a set of 14 capability needs after analyzing the virtual meeting results. HSSAI then developed and distributed an online prioritization tool that responders could use to prioritize among the PR4

[6] Virtual focus group meetings were held using a collaborative Web-based system, allowing participants to review materials simultaneously and provide input and feedback verbally and through posted comments.

[7] The FRRG is distinct from the FRG. The FRRG is a multi-disciplinary group of responders established to provide input and feedback in support of the FRG's development efforts. The IAB is a federally chartered advisory group of state and local emergency responders. Its mission is to "strengthen the nation's ability to prepare for and respond safely and effectively to emergencies, disasters, and CBRNE incidents." For further information, see https://iab.gov.

capability needs. Participants rated the capability needs according to overall priority, criticality of need and other contributing factors.[8]

Simply identifying emergency response capability needs is not sufficient for technology development decisions. It is important to understand the actual capability gaps. These gaps represent the difference between current capability and what responders believe is required to effectively and efficiently complete their tasks and mission. This requires a clear articulation of the baseline capability—what responders have now—and the quantitative and qualitative goals that describe what they believe is needed. To gather initial data on baseline capabilities, HSSAI facilitated discussions with members of the IAB's Strategic Planning Subgroup. Participants reviewed the 14 PR4 capability needs and provided information and data about their current capabilities (technology, policy, procedures and training) available for response operations.

The goal of phase 2 was to translate capability needs into technology objectives. Technologists require an understanding of what is specifically needed before they can pursue new and innovative solutions. They also need to understand the problems that responders are facing and why current capabilities are insufficient. In phase 2, HSSAI conducted a focus group that included emergency responders and technical Subject matter experts to facilitate this understanding and identify RTOs. RTOs translate the operational capability needs into technical terms.[9] Federal, state and local emergency responders with experience in catastrophic incident response and recognized Subject matter experts in fields related to the capability needs participated in the focus group, held in Washington, D.C., in November 2013. Responders described each capability need and explained the operational issues that they face. Technologists translated the needs into RTOs that, as a whole, should address the capability needs.

Technologists are better able to identify a proposed path to address needs if they have a concrete understanding of responder goals for each RTO. HSSAI conducted a workshop in San Antonio, Texas, in March 2014 to capture these goals. Federal, state and local responders participated in a series of facilitated discussions describing both their current capabilities and what they believe is necessary to achieve mission success for each RTO.

The goal of phase 3 was to evaluate the state of science and technology to identify potential technology solutions that meet responder needs. HSSAI conducted a series of in-person and telephone interviews with Subject matter experts who work in fields related to the RTOs. These experts were from national laboratories, government agencies, academia, private industry and standards and professional organizations. HSSAI conducted interviews with several experts in each field to obtain multiple perspectives and inputs. The interviews produced information and data about the state of technology, proposed paths to meet responder goals, associated resource needs and potential barriers.

[8] See Appendix C for a discussion of the PR4 Prioritization Process.

[9] See Figure 4 in the section on Key PR4 Concepts for a more complete definition of key terms used in the development of this plan.

In the fourth and final phase of this effort, HSSAI assessed and integrated the information from responders and Subject matter experts to identify actionable programs for increasing capability. HSSAI also developed technology road maps that illustrate an integrated pathway for capability advancement.

Enduring and Emerging Needs

The first *Project Responder National Technology Plan*, published in 2004, was a unique, multi-disciplinary examination of emergency response capabilities required to respond to catastrophic events. It reflected a comprehensive review of capability needs across the totality of the emergency response mission. Subsequent iterations of Project Responder updated and prioritized those capability needs to reflect changes in the response environment because of a focus on all-hazards response, the introduction of foundational response doctrine, evolving threats and a constrained fiscal environment.

The second and third iterations of Project Responder did not provide recommendations of potential technology solutions to meet the identified needs. There have not been significant changes to the response environment since the PR3 report was published in December 2011. Consequently, another comprehensive review of capability needs was unnecessary. A number of capability needs have endured across all phases of Project Responder. A review of results from the three previous Project Responder efforts indicates that participants consistently rated a number of capabilities as a high priority. Although the threat and response environments have changed over the intervening 12 years, many of the previously identified capability needs and gaps endure. Figure 2 illustrates the continuity in prioritization of some capability needs.

Capability Priorities Across Time[10]

2004 Priorities	2008 Priorities	2011 Priorities
Body protection from all hazards	Command and management	Virtual simulation training
On-scene detection	Communications[11]	Responder location
Remote and standoff detection	Seamless data integration	All-environment communications
Point location and identification	Full-body personal protection	Remote tactical monitoring
Seamless connectivity and integration	Logistics support[12]	Body protection from all hazards
Mass victim decontamination	Mass prophylaxis distribution	Personal Protective Equipment (PPE)-integrated communications
Risk awareness and assessment	Training and exercise programs	Threat detection and monitoring
Mass medical prophylaxis	Mass victim decontamination	Resource availability
Mass casualty medical care management	Responder respiratory protection	Trend and pattern identification
Individual and collective protection	Point location and identification	Hazard identification
Surveillance and information integration	Prioritization and dissemination of threat information	On-scene resource status
Logistics information systems	Credentialing	Casualty location
Threat assessment/data collection/analysis		

Figure 2. Project Responder Capability Priorities, 2001 to 2011

As depicted in this graphic, responders consistently identify body protection, responder location, interoperable communication (voice and data), logistics management and threat

[10] A color coding system is used throughout this report to provide an organizational structure whereby color cues may help the reader understand which topic is being addressed (for example., information related to communications consistently uses red font or shading). Pages 15 to 17 illustrate the coloring assigned to each capability need.

[11] There were three capability needs related to communications in the 2008 *Project Responder Review of Emergency Response Capability Needs*.

[12] There were two capability needs related to logistics support in the 2008 *Project Responder Review of Emergency Response Capability Needs*.

assessment as priorities for capability advancement. HSSAI chose these enduring needs, and the others identified as high priority during the PR3 effort, as the starting point in identifying capability needs to address in PR4.

The other high-priority needs from PR3 include:

- Readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response
- The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time
- Communications systems that are hands-free, ergonomically optimized and can be integrated into PPE
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time
- The ability to rapidly identify hazardous agents and contaminants
- The ability to remotely scan an incident scene for signs of life and decomposition to identify and locate casualties and fatalities

It is also important to capture emerging needs—those that have arisen or increased in priority because of technological advancement, social or cultural change or other drivers. While the response environment has not changed significantly, changes and innovation in other areas have the potential to influence changes in response doctrine and operations. HSSAI identified two emerging needs from the responder inputs during the virtual focus group meetings:

- The ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into incident command and operations
- The ability to identify, assess and validate emergency-response-related software applications

The first of these emerging needs was identified during PR3 but was not ranked among the highest-priority needs. The second emerging need was newly identified by responders in PR4.

Figure 3 illustrates the sources of the final set of 14 PR4 capability needs:

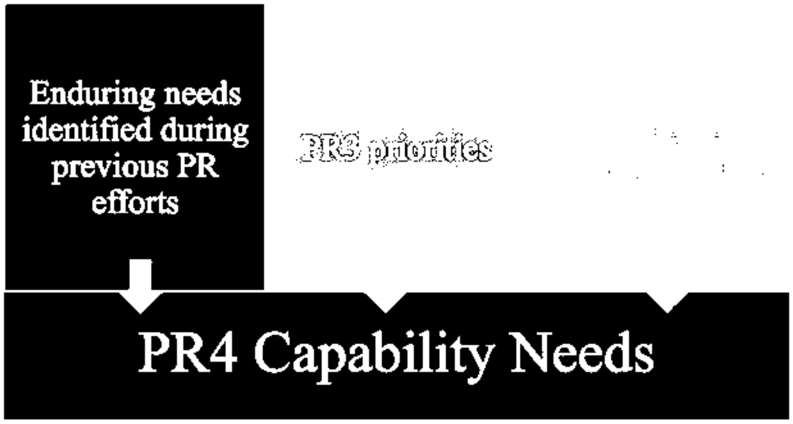


Figure 3. PR4 Capability Needs

Key PR4 Concepts

This plan is based on the concepts defined in figure 4. These concepts provide a structure to understand the capabilities needed for catastrophic incident response. The structure is hierarchical, with one level of the structure providing inputs to the next.

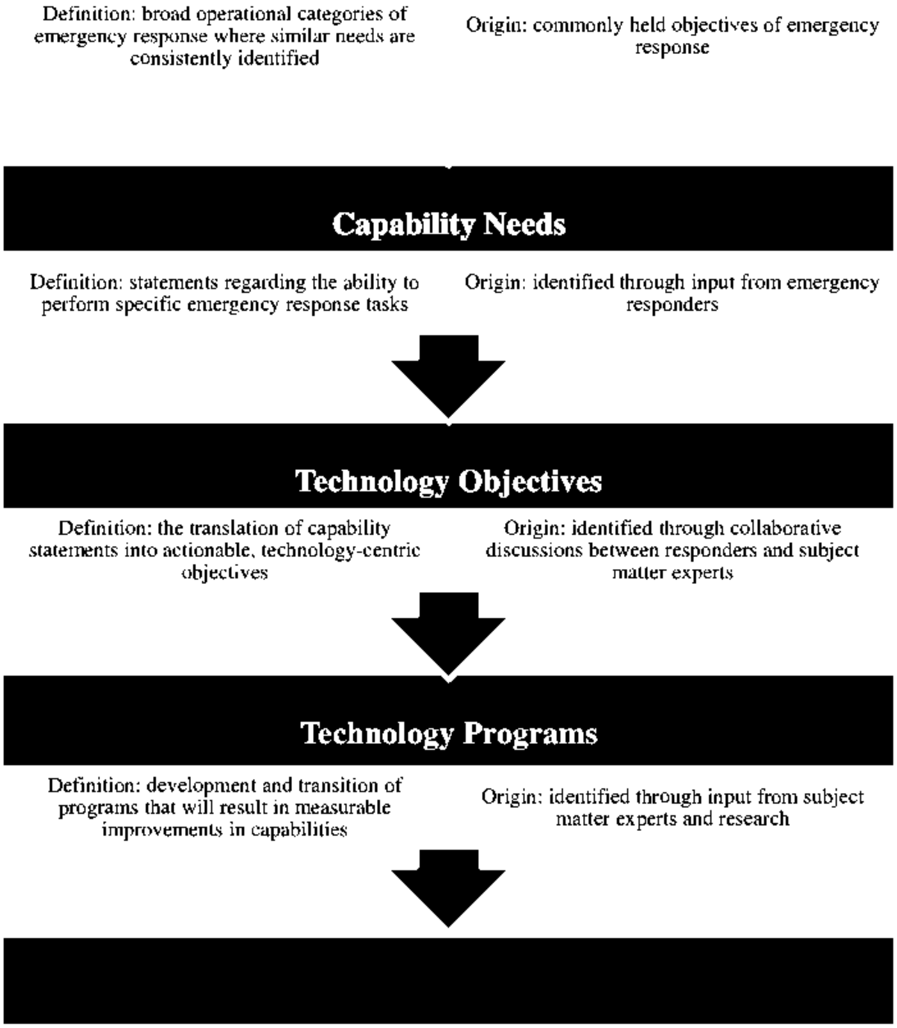

Definition: broad operational categories of emergency response where similar needs are consistently identified
Origin: commonly held objectives of emergency response
Capability Needs
Definition: statements regarding the ability to perform specific emergency response tasks
Origin: identified through input from emergency responders
Technology Objectives
Definition: the translation of capability statements into actionable, technology-centric objectives
Origin: identified through collaborative discussions between responders and subject matter experts
Technology Programs
Definition: development and transition of programs that will result in measurable improvements in capabilities
Origin: identified through input from subject matter experts and research

Figure 4. Key Concepts—Definitions and Origins

Capability domains represent broad operational categories of emergency response where similar needs are consistently identified. These domains provide an organizational construct to allow structured discussion around capabilities instead of disciplines or jurisdictions. The capability domains in this plan were originally described and defined in the PR3 report.[13]

The domains are as follows:

- *Situational awareness:* the capability to provide and distill specific knowledge concerning emerging threats, hazards and conditions in a

[13] The capability domains were derived from the FEMA Core Capabilities List, previous Project Responder reports, Presidential Policy Directive–8 and other relevant documents.

timely fashion to support incident management decisions across all phases of catastrophic incident response

- *Communications:* the capability to seamlessly and dynamically connect multiple persons/entities and convey meaningful and actionable information to all relevant parties

- *Command, control and coordination (C3):* the ability to identify incident priorities, allocate scarce resources and exchange relevant information to make effective decisions in a stressful environment

- *Responder health, safety and performance:* the ability to identify hazards to public safety personnel and develop appropriate mitigations to reduce morbidity and mortality associated with response activities

- *Logistics and resource management:* the capability to identify, acquire, track and distribute available equipment, supplies and personnel in support of catastrophic incident response

- *Casualty management:* the capability to provide rapid and effective search and rescue, medical response, prophylaxis and decontamination for large numbers of incident casualties and identify appropriate sheltering and transportation options

- *Training and exercise:* the ability to provide instruction on necessary skills for catastrophic incident response and coordinate and practice implementation of plans and potential response prior to an incident

Capability needs are statements that describe an essential ability required to perform a critical response function. They are identified through data-gathering efforts with the emergency response community. Participants in the virtual focus groups vetted the list of capability needs, examining each of the 40 needs identified during PR3 and suggesting emerging needs. Responders used an online prioritization tool to rate the capability needs according to several factors. Each of the capability needs fits into one of the capability domains.

RTOs translate the capability statements into actionable, technology-centric objectives. An RTO identifies a high-level technology solution (or part of a solution) for a capability need. HSSAI developed draft RTOs using data gathered during the focus group held in November 2013. Subject matter experts who participated in the data-gathering interviews vetted the RTOs and provided input on ongoing development efforts, technical challenges, potential technology programs and associated resource requirements. The 42 RTOs in the *Findings* section are described in terms of relevance, responder requirements, a summary of the state of technology, anticipated benefits and potential challenges or barriers to improving the capabilities.

Technology programs describe potential solutions for each RTO. The subject matter experts who participated in the interview process suggested programs to address the operational requirements articulated by the responders. The technology programs in this plan are listed in the *Path Forward* section of each RTO and illustrated in the technology road maps.

Participation

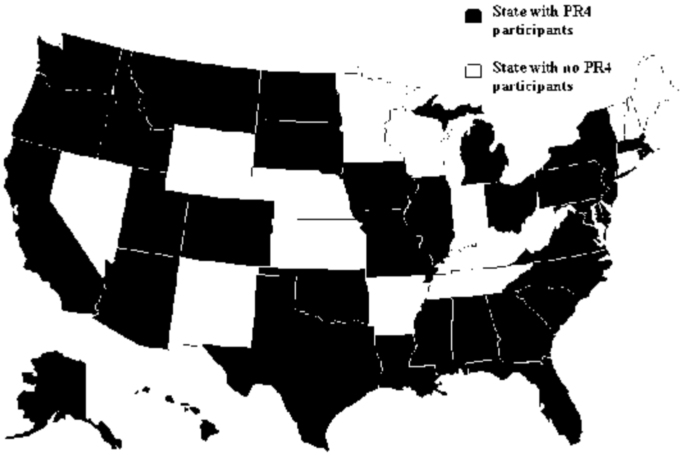

■ State with PR4 participants
□ State with no PR4 participants

Figure 5. Geographical Distribution of PR4 Participants

It has been a fundamental component of the Project Responder effort over all four iterations to involve responders—the men and women who will ultimately be responsible for responding to catastrophic incidents—in the identification and prioritization of capability needs and the development of proposed technology paths. Actions taken to address gaps in capability require the involvement of responders to identify potential impacts on operations. Development of technology solutions without responder input can result in wasted resources and tools or equipment that go unused because they do not meet operational requirements. While responders may not be able to identify technology solutions, they are able to describe in detail what they need to be able to execute their mission successfully. It is important to obtain this input from a set of participants diverse in terms of discipline, size and location of jurisdiction and level of government. Capabilities for emergency response vary significantly across the country and incorporating multiple perspectives helps ensure that the overall level of capability is understood.

HSSAI identified responders on the basis of their participation in the IAB and FRRG, previous participation in the Project Responder process, and experience with response to or management of large-scale incidents, as well as recommendations from some of the nation's most experienced and well-respected responders. Participants from traditional and nontraditional disciplines participated in the PR4 process, including the fire service, law enforcement, emergency medical services (EMS), emergency management, urban search and rescue, public health, public utilities and transit services. Federal, state and local responders from 34 states and the District of Columbia participated in the PR4 process.[14]

[14] This number does not include those responders who participated in the prioritization process. All members of the IAB and FRRG received an invitation to the online tool. Basic demographic information

HSSAI gathered input from Subject matter experts from national laboratories, government agencies, academia, private industry and standards and professional organizations who work in technology fields related to the RTOs. A group of 11 Subject matter experts participated in the focus group and more than 40 participated in the interview process. HSSAI identified Subject matter experts through review of technical documents, journals and conference proceedings; open-source research of available products; and recommendations by other experts. A list of all PR4 participants can be found in Appendix D.

Scope

This plan describes proposed development paths to improve high-priority capabilities for emergency response to catastrophic incidents. Catastrophic incidents include natural disasters and man-made events (terroristic and accidental) that exceed the capabilities and resources of a local jurisdiction or region. Project Responder is not focused on daily response activities (for example, fighting a house fire or conducting an investigation).[15]

In this plan, HSSAI identified science- and technology-based products and solutions (in other words, equipment, knowledge products, and standards) that can address responder needs. When applicable, this plan mentions potential non-technology solutions but does not address them in detail.

The Subject matter experts who participated in the focus groups and interviews estimated costs associated with the technology programs. HSSAI did not conduct an independent cost development effort or perform a formal cost and benefit analysis. In addition, HSSAI did not do a detailed assessment of technical risks associated with these programs.

The rationale and methodology for this plan were based on a capabilities-based planning approach. According to a RAND study for the Department of Defense, "[c]apabilities-based planning is planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice."[16] Capability-based technology planning begins by asking the operators—the users of technology—what they need to do that they cannot do today. This planning method focuses on the functions that need to be performed and provides technologists with a clear set of prioritized operational goals toward which they can direct their efforts. One limitation of engaging operators is that each has personal biases that may impact their input. To mitigate this concern, HSSAI used experienced

was collected from the 129 responders who participated, but their results were anonymous. Therefore, it is not possible to determine the number of responders who also participated in another PR4 event.

[15] Although Project Responder is not focused on the capabilities needed for daily response activities, it is important that new technologies that are developed for emergency response are also integrated into daily use equipment whenever possible.

[16] Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation*, prepared by RAND National Defense Research Institute for the Office of the Secretary of Defense.

facilitators during the focus group and workshop discussion sessions and invited participants from multiple disciplines, agencies and jurisdictions to obtain varied perspectives.

HSSAI attempted to identify both the appropriate Subject matter experts and ongoing technology initiatives for the data-gathering effort. However, not all invited technologists were able to attend, and other experts or technology programs may not have been identified through HSSAI's research. Further, it is possible that some research and development in the areas addressed by the RTOs is classified and therefore cannot be included in this plan.

In the first Project Responder report (published in 2004), leading responder associations were given the opportunity to review and endorse the findings. This endorsement is valuable because of the implied concurrence with the study findings by a much larger group of responders. The period of performance associated with PR4 did not allow for the independent review and validation by these associations before the final plan was due to DHS. However, HSSAI did invite members of key associations to participate and obtained their input during the data gathering phases of this effort.

FINDINGS

This section details the findings from the PR4 effort. First, it identifies the PR4 capability needs by domain and summarizes the results of the prioritization process. Second, it describes some crosscutting considerations for technology development. Third, it describes each of the 42 RTOs that correspond with the PR4 capability needs.

Project Responder 4 Capability Needs

There are 14 capability needs for emergency response to catastrophic incidents that are addressed in this plan. As described in the *Enduring and Emerging Needs* section above, the capability needs were identified through analysis of capability needs consistently identified throughout all phases of Project Responder, other high-priority needs identified in PR3 and emerging needs suggested by emergency responders. The 14 needs are listed below. They are depicted in colored boxes by capability domain. This color coding system is used throughout this report to provide an organizational structure whereby color cues may help the reader understand which domain is being addressed.

Situational awareness is defined as the capability to obtain and distill specific knowledge concerning threats, hazards and conditions in a timely matter to support incident management decisions across all phases of a catastrophic incident response.

The ability to know the location of responders and their proximity to risks and hazards in real time

The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time

The ability to rapidly identify hazardous agents and contaminants

The ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into incident command operations

Communications is defined as the capability to seamlessly and dynamically connect multiple persons or entities and convey meaningful and actionable information to all relevant parties.

[redacted]

Communications systems that are hands free, ergonomically optimized and can be integrated into PPE

Command, control and coordination is defined as the ability to identify incident priorities, allocate scarce resources and exchange relevant information to make effective decisions in a stressful environment.

The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time

The ability to identify trends, patterns and important content from large volumes of information from multiple sources (including nontraditional sources) to support incident decision-making

The ability to identify, assess and validate emergency-response-related software applications

Responder health, safety and performance is defined as the ability to identify hazards to public safety personnel and develop appropriate mitigations to reduce morbidity and mortality associated with response activities.

[redacted]

Logistics and resource management is defined as the ability to identify, acquire, track and distribute mission-specific equipment, supplies and personnel in support of catastrophic incident response.

The ability to identify what resources are available to support a response (including resources not traditionally involved in response), what their capabilities are and where they are, in real time

The ability to monitor in real time the status of resources and their functionality in current conditions

Casualty management is defined as the ability to provide rapid and effective search and rescue, medical response, prophylaxis and decontamination for large numbers of incident casualties and identify appropriate sheltering, transportation and destination options.

[redacted]

Training and exercise is defined as the ability to provide instruction on necessary skills for catastrophic incident response and coordinate and practice implementation of plans and potential response prior to an incident.

> Readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response

Previous Project Responder efforts used a technique called Q methodology to prioritize the capability needs arising from the facilitated discussions. This methodology enables a group of participants to rank order a large number of opinion statements relative to each other. While Q methodology was well suited to rank order the larger number of capabilities identified in previous Project Responder iterations, it is less suitable for understanding the underlying factors necessary to prioritize a smaller subset of enduring and emerging capability needs. For PR4, HSSAI sought to identify and understand the specific factors that make each capability a priority. HSSAI asked emergency responders to identify the factors that cause one capability to be ranked higher than another. The factors were then used as the foundation to develop an online tool. The online tool provided a uniform assessment path for responders to follow when they evaluated each capability statement.

In the prioritization tool, responders were asked several questions, and the responses to each question were based on a seven-point scale. The full question set included the following questions:

- How would improvements in this capability improve *responder safety*?
- How would improvements in this capability improve the *safety of the affected population*?
- How would improvements in this capability improve the *ability to mitigate incident consequences*?
- How would improvements in this capability improve *decision-making for incident management*?
- Can improvements in this capability *be used in multiple types of incidents*?
- Overall, how important a priority is this capability?

Participants were also asked to rank what they perceived to be the three most critical capabilities and the least critical capability. The prioritization tool was distributed to all members of the FRRG and IAB. It was available over a two-week period. More than 125 responders participated, with a 90 percent response rate for each question. The results from the prioritization process indicate that six needs rank the highest in terms of overall priority. Figure 6 presents the overall priority ranking of the top six capability needs.[17]

[17] Appendix C provides more detail about the development and results of the PR4 prioritization process.

Capability Need	Mean Score
The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)	6.3
The ability to know the location of responders and their proximity to risks and hazards in real time	6.1
The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time	6.0
The ability to rapidly identify hazardous agents and contaminants	5.9
The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time	5.7
Protective clothing and equipment for all responders that protects against multiple hazards	5.4

Figure 6. Capability Needs by Overall Priority Ranking

HSSAI also examined the criticality rankings of the capability statements. This assessment yields results that are similar to the rankings of overall priority. Three capability needs received significantly more votes than the other capability needs. Figure 7 presents the criticality ranking of the capability needs.

Capability Need	Number of Votes
The ability to know the location of responders and their proximity to risks and hazards in real time	85
The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)	70
The ability to detect, monitor, and analyze passive and active threats and hazards at incident scenes in real time	39

Figure 7. Capability Needs by Criticality Ranking

The same capability needs are consistently ranked highest given the two ranking methods, with the primary difference being that the highest ranked swap the first and second positions. Although the *ability to communicate with responders in any environmental conditions* is ranked higher in overall priority, responders assessed the *ability to know the location of responders and their proximity to risks and hazards in real time* as more critical to address first. Overall, the consistency of these rankings indicates their degree of importance to the responder community.

Considerations for Technology Development and Adoption

Participants in the PR4 process, both responders and other Subject matter experts, identified a number of issues that should be taken into consideration when reviewing the RTO descriptions. These issues address overarching or crosscutting factors that affect both the response community and those interested in pursuing the proposed programs described in this plan.

Big data. Addressing the capability needs identified in this plan may create significant big data challenges for the response community. Big data problems exist when large amounts of data are collected from multiple sources and the data sets become too large or complex to transmit, filter and process in a timely manner. Many of the devices or systems discussed in this plan will create data streams that must be transmitted in real time to incident command to be useful. Telemetry data showing the location of hundreds of responders on the incident scene, for example, will be less useful if the data transmission overloads existing communications infrastructure and is not received in real time. Responders and the population may be in jeopardy if sensors that detect the presence of hazardous agents cannot transmit pertinent information in real time. This issue is exacerbated during emergency response to catastrophic events because network connectivity and available bandwidth can be severely hampered. Big data problems persist once information is received by incident command. Numerous advances in technology will be useless if the transmitted information is so complex or extensive that it cannot be processed by incident command or the appropriate responder. The big data challenge transcends many of the technology programs and can impede the improvements promised by these new tools.

Crosscutting requirements. Each RTO described below includes a list of responder goals. These goals describe attributes that responders believe are necessary as part of the new tools, devices, systems and platforms developed to address the PR4 capability needs. There are a number of attributes that responders mentioned during nearly every RTO discussion. Instead of listing these goals repeatedly, they are addressed here as a set of base requirements:

- *Power source* – Availability of power sources can be a significant issue in catastrophic incident response, as the nature of the incident can damage or destroy the power infrastructure. Responders need tools that can utilize multiple power sources (for example, accessing the power infrastructure of on-scene buildings, generators and batteries). Portable power systems should be long-lasting and lightweight and should not use proprietary interfaces or components.
- *User interface* – The interaction between the responder and the device must be intuitive and easy to use. Responders do not want complex or cluttered displays. Components should be clearly labeled and the system should be based on a logical construct derived from responder requirements.
- *Cost* – Cost is a significant issue for the response community. The current fiscal environment dictates that budgets for public safety agencies are tight and

available funding for capital purchases is limited. Affordability should be a key factor during technology development, including initial costs and recurring maintenance and calibration.

- *Daily use* – Responders do not want a separate set of equipment that is only used during response to large-scale incidents. Responders may not have the time to re-familiarize themselves with equipment that has specialized functionality and is not used on a daily basis. Tools and systems developed to address the PR4 capability needs should be, to the extent possible, used during routine operations.
- *Training* – Training should be clear and concise. When possible, and appropriate, training should be available via Web-based instruction or provide a train-the-trainer option, where one staff member can learn to teach others about the specific topic.

Spiral development. The responder goals described for each RTO do not constitute a minimum set of requirements that must be met before new tools, devices, platforms or systems can be released. Responders stated that they would prefer incremental, continuous advancement over waiting several years for a piece of equipment that meets all of the stated goals at the same time. Not only do requirements change as the response environment evolves, but even minor advancements in capabilities can improve response operations. Likewise, some of the goals described below are quantitative in nature. They describe a specific weight or distance. Responders do not want these specifications to be construed as a minimum requirement. Being able to locate responders indoors to within 10 feet (instead of the one-foot goal described below) still represents a significant improvement over what is available today. Quantitative goals should also be subject to the spiral development methodology.

Reach goals. Some of the goals described below can be considered "reach goals," with quantitative criteria that exceed what technology can deliver today. During the workshop discussions, responders were asked to describe the attributes that they believe are necessary to complete their tasks and missions effectively, without consideration for cost or technical feasibility. The goals represent what responders believe that they need in terms of capability. As with the discussion on spiral development, these reach goals should be viewed as goals, not as minimum requirements before new products are released to the response community. As technology continuously advances, what was previously infeasible may become possible and the reach goals may someday be achievable.

Responder involvement. The criticality of involving the emergency response community during all phases of technology development should not be understated. Too often, products are developed without a clear concept of operations or understanding of operational realities. This results in tools and equipment that do not meet the demands of the user community and potentially wasted investment. Responders cited examples where buttons were too small to push while wearing gloves, devices were not ruggedized to withstand heat and humidity or responders were put in greater danger when trying to deploy a device. Responders can provide iterative input and feedback from requirements generation through testing and evaluation.

Resistance to change. The response community as a whole can be resistant to change. Many of the goals described in this document bring the capabilities of the response community in line with what is already available in other fields. However, responders often like to do things the way they have always been done. Responders reported that there is an internal struggle within the response community, and perhaps within each individual responder, between honoring tradition and culture and wanting improvements in capabilities. This struggle is not limited to only one discipline; there are multiple examples where advances in technology, even those that could improve responder safety, are rejected because they conflict with tradition. One important consideration for technology developers is that they will not be able to force change. Developers and manufacturers need to understand their customer and the motivations for why things are currently done as they are. Responders rely on whiteboards and grease pencils because that is what has worked in the past (and in some cases because that is what they could afford). The response community needs to embrace technology, but this may not be an easy sell. A younger generation of responders may embrace technology to a much greater extent, but new technologies introduced now may have to demonstrate not only that they can withstand the extreme conditions on the incident scene, but also that they can measurably improve capability.

Personnel qualifications. Greater use of and reliance on technology may mean that personnel qualifications may change or new staff positions may be necessary. Currently, many public safety agencies do not have a separate staffed position focused on information technology (IT). Often, IT work is assigned as an additional duty to a responder interested in the field, or IT issues are addressed through support contracts with outside firms. However, the need for an on-site, skilled, and dedicated IT staff becomes more acute as the number of networked devices on the incident scene increases.

Changes in doctrine. In addition to potentially changing the necessary skill set of public safety agencies, many of the technology advancements identified in this plan have the potential to notably change the tactics, techniques and procedures (TTP) used in emergency response today. For example, being able to remotely detect the location of casualties may change the current practice of sending out separate teams to search for trapped victims. Likewise, the ability to conduct virtual training and exercises may reduce the number of full-scale exercises that need to be held. A larger, multi-disciplinary body should periodically assess how TTP can evolve as a result of advances in technology.

Project Responder 4 Response Technology Objectives

Each of the 42 RTOs identified during the PR4 effort is described below. The RTOs are grouped by domain, and each domain is a separate section or chapter. The color coding system used above continues here (for example, all of the RTOs pertaining to situational awareness have blue shading and text boxes) to provide the reader with organizational cues.

Each domain chapter contains an introduction identifying the corresponding capability needs and describing each need as it applies to catastrophic incident response. Each RTO contains a number of components:

- *Relevance* – This paragraph describes how the RTO addresses a necessary component of catastrophic incident response.
- *Current capability* – This paragraph describes the equipment and resources that response agencies currently have available.
- *Responder goals* – These bullets list responder-articulated attributes that, taken as a whole, describe the increase in capability that responders believe is necessary.
- *State of technology* – This section provides a qualitative description of existing or proven capabilities in this or related areas, as well as ongoing development efforts.
- *Potential challenges* – These bullets identify conceivable technology and non-technology barriers that could inhibit development or operational implementation.
- *Anticipated benefits* – This graphic illustrates expected operational improvements associated with meeting responder goals.

Responders described current capability and identified goals over the course of multiple focus group meetings, a workshop and several other data-gathering sessions. Subject matter experts described the state of technology and suggested annual milestones and estimated potential costs during the interview process. HSSAI did not develop costs independently, and further refinement of costs should be among the initial steps taken during the acquisition process.

HSSAI gathered much of the information described below, including the current capability and state of technology sections in particular, from an amalgamation of sources. Specific citations are provided for all DHS and other efforts funded by federal agencies. For commercial programs and products, HSSAI chose to describe the state of technology in more general terms to avoid the perceived endorsement of specific products or manufacturers.

Situational awareness is defined as the capability to obtain and distill specific knowledge concerning threats, hazards and conditions in a timely matter to support incident management decisions across all phases of a catastrophic incident response.

There are four capability statements in this domain:

[redacted]

Since Project Responder began in 2001, emergency responders have consistently stated there is a need to precisely identify the location of responders in real time. Incident commanders and team leaders need a tool that displays the location of responders and their proximity to threats and hazards. During a catastrophic incident, responders may operate over an extensive geographic area without adequate knowledge of the hazards and threats. The ability to geolocate responders (identify their location on the incident scene tied to latitude, longitude and altitude coordinates or area-specific designations such as a street address), in all environments (in other words, indoors, outdoors and maritime), combined with simultaneous awareness of incident hazards, could greatly improve the safety of emergency responders. As an example, precise geolocation of responders may have prevented the catastrophe that occurred in Arizona on June 30, 2013, when 19 Granite Mountain Hotshot crewmembers were killed after being overtaken by an approaching wildfire threat. Incident command did not have adequate situational awareness or the ability to communicate with the crew to alert them of the impending hazards.

Subject matter experts identified five RTOs that correspond with this capability:

- Indoor (Above and Below Ground) Responder Geolocation
- Outdoor Responder Geolocation
- Maritime (Above and Below Water) Geolocation
- Infrastructure Standards for Technology Integration
- Rapid Building Characterization, Generation and Display

The ability to rapidly identify hazardous agents and contaminants

Upon arriving at an incident scene, responders may have little or no awareness of the hazardous agents or contaminants that may be present. This lack of awareness places responders at increased risk of exposure to a range of threats, including unknown toxins, biological agents or contaminants, during response operations. Catastrophic incident response only amplifies this issue, as the scale and scope of a catastrophic incident increase the likelihood of numerous hazardous agents on the scene. Even minimum exposure to many of these agents can cause significant health concerns. Responders need the ability to detect hazardous agents remotely and understand pertinent information regarding protective actions or treatments.

Subject matter experts identified three RTOs that correspond with this capability:

- Improved Standoff Detection and Identification of Multiple Hazards
- Multi-Sensor Integration and Analysis
- Risk Assessment and Decision Support to Command

The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time

Threats and hazards during a catastrophic incident can change rapidly. Dangers detected at incident onset may increase, decrease or evolve over time, while new and unexpected hazards can emerge. Both passive and active threats and hazards can exist simultaneously on incident scenes, particularly during catastrophic incidents, increasing the potential risk to civilians and responders. Responders need the capability to continuously detect, characterize, monitor and analyze threats and hazards. On-scene, rapid detection and timely alert of changes to the threat environment is critical for responders to take timely protective actions. Broad understanding of threats and hazards, and real-time changes to them, would inform response operation decisions.

Subject matter experts identified three RTOs for this capability:

- Remote Monitoring of Threats and Hazards
- Combined Effects Assessment
- Automated Red-Force Tracking[18]

The ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into incident command operations

Emergency managers rely on multiple information inputs to make decisions. These inputs include field observations, sensor data, model outputs, images and video, media reports, databases and other sources. With advances in technology, responders are exploring ways to integrate nontraditional sources of valuable data (for example, sensors attached to infrastructure, road cameras, social media data) into decision-making processes. Responders noted the increasing importance of information from nontraditional sources and the need to integrate these information streams into a common operating picture. Although responders see value in systems that could aggregate and analyze nontraditional information sources, they also emphasized the need to verify information. To be actionable, responders need to be confident that data has been validated and obtained from a verified source. At present, nontraditional data are not fully incorporated into incident command common operating pictures for decision-making.

[18] Red forces denote a specific threat or hazard and could be a person or persons (for example, active shooters or suspects), or an item such as a weapon or an explosive device.

Subject matter experts identified two RTOs that correspond with this capability:

- All-Source Collection and Integration of Data
- All-Source Information Validation

Indoor (Above and Below Ground) Responder Geolocation

Relevance: Responders frequently operate inside buildings, underground (for example, basements, subway systems) and under debris and rubble. Responders may not have adequate knowledge of their own location or those of other responders indoors, especially if the environment is impaired by smoke or lack of light. Moreover, incident commanders who are managing the response may not know the location of personnel deployed on-scene. These circumstances become exacerbated during a catastrophic incident when individuals are responding from multiple jurisdictions, further degrading situational awareness. Incident command needs the ability to locate, evacuate or rescue at-risk or trapped responders, identify personnel at key locations and notify responders if they are in proximity to threats and hazards. This requires precise location of responders on-scene. Geolocation is the geographical position of an object, usually defined by latitude, longitude and altitude. Knowing the coordinates of responders and their proximity to hazards is critical for responder safety.

Current Capability: Currently, most agencies do not have the capability for real-time automated geolocation of responders on the incident scene. Responders often transmit their location coordinates verbally, using hand-held radios. Real-time geolocation requires the responder to wear a device that broadcasts global positioning system (GPS) coordinates. GPS works by constantly transmitting a signal to satellites in orbit to calculate a position. These signals contain metadata on the exact time the signal was transmitted and where the satellite was when the signal was sent. The device then calculates the time it takes for four or more of these signals to reach the device from a satellite to trilaterate the location.[19] These signals are not powerful enough to penetrate building walls or even a thin piece of metal, which makes indoor and below ground geolocation very difficult, even with the most sophisticated technology available. Even if a responder knows his or her own GPS coordinates, they must then be transmitted in real time to incident command. Incident commanders generally rely on the last known position (as communicated by the responder or approximated based on tasking) to identify the location of personnel in GPS-denied environments, such as inside buildings. In an emergency situation, it is possible to "ping" the smartphones carried by many responders to identify their last known position. However, because GPS signals are obstructed indoors, this position may be temporally and geographically out of date. The

[19] In addition to Standalone GPS, described above, Assisted GPS (A-GPS) also represents a capability to support geolocation. A device can report multiple data points (for example, the location of Wi-Fi points, satellite data, other provider infrastructure) back to the network. The carrier can use this information to identify the approximate location of the device. Similarly, the carrier can provide wireless phase locations to public safety agencies to support the location of devices. These capabilities are currently available, but are not used frequently by response agencies in time-sensitive situations.

newest generation of land mobile radio systems can automatically transmit a GPS signal at a rate determined by the system administrator if connected to a digital trunking system.

Responder Goals:

- Accurate geolocation of responders to within one to three feet for x, y and z coordinates
- Real-time and recurring transmission of responder location to incident command
- Graphic display of the location of all responders on the incident scene
- Integrates with graphic display of on-scene hazards and threats
- Integrates with 3-D display of buildings and structures to identify the room or specific area in which the responder is located
- Integrates with other information about the responder's condition (in other words physiological data, personal alert safety system [PASS] alarm activation)
- Integrates with common electronic situational awareness tools
- Location transmitters should be ruggedized, simple and transparent and users should not be able to turn them off
- Integration of transmitters into PPE or other existing equipment with minimal or no net weight gain for the responder[20]
- Size, weight and power (SWP) suitable for responder operating conditions
- Assumes no prior knowledge of the environment (for example, no maps available or prior information about the building)
- Incorporates a confidence level to indicate the accuracy of location
- Affordable to outfit entire workforce
- Caches data when connectivity is offline and automatically forwards when connection is restored

State of Technology: Significant advances have been made with regard to responder location and hazards sensors, but there are still significant limitations with existing technologies. It is not currently possible to pinpoint a responder's location within one foot (the ideal metric identified by responders). Indoor geolocation, particularly when the subject is underground, is a harder technology issue to address than outdoor geopositioning, largely due to the lack of GPS accessibility indoors.

[20] PPE is defined here to include all garment layers and associated protective equipment (for example, a self-contained breathing apparatus) designed to provide body and respiratory protection for emergency responders.

Technologies said to be state of the art work in controlled testing environments but experience issues when operating in realistic emergency-response-like conditions. For example, accuracy decreases when individuals wearing geolocation devices perform actions that are common during an incident such as crawling, climbing or even jumping. Ongoing research continues to advance the state of the art, but most systems available today are considered to have a relatively low readiness level.

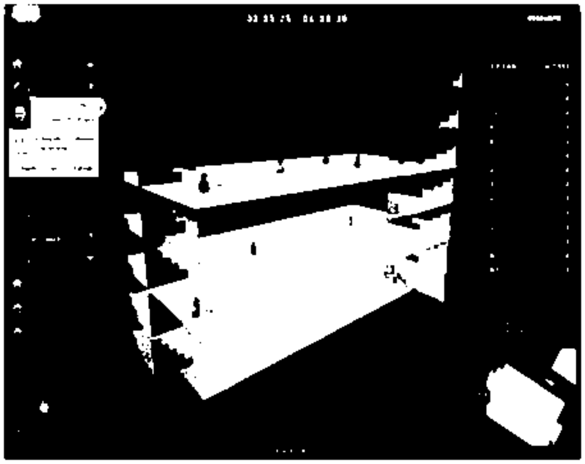


Figure 8. GLANSER – Indoor Location System

The Geospatial Location Accountability and Navigation System for Emergency Responders (GLANSER), largely supported by DHS, is being developed to provide geolocation for emergency responders.[21] GLANSER includes a geospatial locator unit that fuses information from inertial, barometric pressure, Doppler velocimeter and radio frequency (RF) ranging to compute the responder's 3-D location. That information is sent to the incident commander base station, which could be mounted on a responder apparatus, such as a fire truck, over an ad-hoc mesh radio network. The commander can then view a two-dimensional or three-dimensional display of a responder's location and status.

Other organizations, including the Department of Defense (DOD), also rely on GPS technology in difficult operating environments such as inside buildings, in urban canyons, under dense foliage, underwater and underground. The Defense Advanced Research Projects Agency (DARPA) is currently funding the Adaptable Navigation Systems (ANS) program.[22] As with GLANSER, the goal is to establish GPS-like information irrespective of the operating environment.

Industry has developed location systems that could be ready for distribution with minimal additional time and funds. These are primarily proximity systems, which provide the general vicinity of a responder's location based on networked sensor data from the responder and from other nearby responders. Other commercial providers are transitioning capabilities developed for the U.S. military, using inertial measurement units (IMUs) affixed to the user's footgear for localization in GPS-denied environments.

[21] "GLANSER: A Scalable Emergency Responder Locator System," Worcester Polytechnic Institute Workshop, 2011, http://www.wpi.edu/Images/CMS/ECE/GLANSER_-_WPI_PPL_2011_-_AmitKulkarni-Aug1(1).pdf.

[22] "Adaptable Navigation Systems", DARPA: Strategic Technology Office, last updated: n.d., http://www.darpa.mil/Our_Work/STO/Programs/Adaptable_Navigation_Systems_(ANS).aspx.

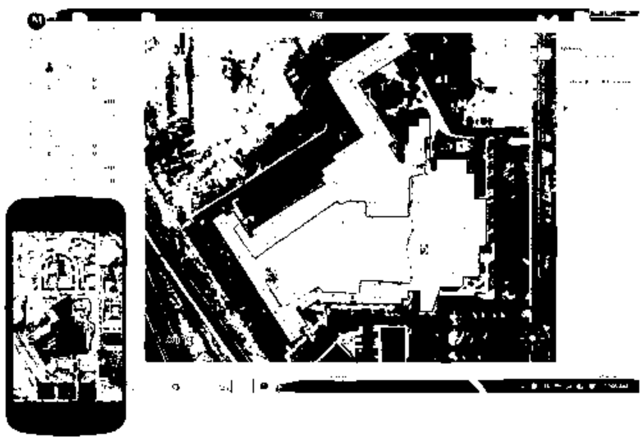


Figure 9. Graphic Display of Responder Location and movement

Research is also ongoing to identify other innovative methods for indoor geolocation, such as Wi-Fi fingerprinting. This approach measures the signal strength of nearby Wi-Fi networks in range along with cartographic knowledge of the network and calculates a relative position. The accuracy of such systems depends on various factors such as walls and the number of people in the room also using Wi-Fi. Currently, the precision of this type of technology can be as good as three meters when there is sufficient Wi-Fi infrastructure and the facility has been pre-mapped. It also has some of the same affordability issues as other approaches and assumes there are available Wi-Fi networks nearby. In the absence of available networks, the technology is ineffective.

Software is currently available to create point-to-point encryption for data, chat, photo transfer, location data and voice communications. The software uses existing smartphone hardware for cellular, GPS and atmospheric sensors (for example, air-pressure changes) to determine geolocation. The use of external sensors (either tethered or wireless) can be integrated to improve location accuracy or report personnel well-being. The software has an alert capability that can notify other personnel, as well as display the alert within a common operating picture (COP). The alert can provide location data, and the transmission of personnel vital information is in development. The alert is manually activated but could be automatically triggered by predetermined criteria (for example, heart rate too high, oxygen saturation levels too low). The software operates over Wi-Fi networks (including mesh) and cellular data, from 2G Edge up to long-term evolution (LTE).

Although multiple products are in development and have shown advancement toward responder geolocation requirements, there are still significant tradeoffs with each type of technology being used. Some of the limitations that are being addressed include:

- *Radio frequency* – Fundamental technological problems include reflection and the significant signal interruption caused by barriers and construction materials such as metal. Addressing this issue is essential if a solution uses RF.
- *Inertial navigation* – Small inertial sensors (for example, accelerometers or gyroscopes) that are affordable to responders currently do not have low enough drift to allow precise geolocation based on inertial sensors alone. The goal is to make small, affordable sensors that have the same performance outcomes of

existing sensors that cost thousands of dollars. To this end, DARPA has established the Micro-Technology for Positioning, Navigation and Timing (Micro-PNT) program.[23] The goal of this program is to develop technology for self-contained, chip-scale inertial navigation and precision guidance for munitions, as well as for mounted or dismounted warfighters. This program addresses size, weight, power and cost concerns and may ultimately allow for the development of a single unit that comprises all necessary devices (for example, clocks, accelerometers and gyroscopes).

- *Low-frequency signals* – These signals can be used to bypass the issue of other high-frequency technology. However, construction materials such as wiring and pipes in a building may produce false readings and throw off the device. In addition, power line noise, caused by sparking or arcing utility pole hardware, is usually most disruptive to lower frequencies.
- *Video* – Video data can be used to sense where an individual is located in a building. However, it has varying levels of effectiveness, particularly in darkness or smoke-filled environments. Research is ongoing to use infrared technology to improve accuracy in these conditions.

A recent influx of indoor responder location technologies has raised concerns among the standards development community. Many of these technologies carry very precise accuracy claims, but when placed in conditions designed to mimic response environments, they do not perform to the levels asserted. As a result, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 18305 standard was drafted to address requirements for indoor responder location and tracking systems. For this standard, "indoor" responder location is defined as any environment where there is no "line of sight to the sky." Under this definition, responders working within or under rubble piles would qualify as "indoor," even though some response entities would classify such activity as "outdoor" since there is no standing structure.

ISO/IEC 18305 is still in the development phase, currently under ballot for validation from the response community. Final publication of this standard is expected sometime in 2015; however, the standard is already in use in some European nations. Once finalized, ISO/IEC 18305 will be the first standard to address responder location systems and will join only a handful of other standards related to location and tracking (including a National Institute of Justice standard on offender tracking).

[23] "Micro-technology for Positioning, Navigation, and Timing." DARPA: Microsystems Technology Office, last updated, n.d., http://www.darpa.mil/Our_Work/MTO/Programs/Micro-Technology_for_Positioning,_Navigation_and_Timing_(Micro-PNT).aspx.

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

- There is a correlation between the size, cost and accuracy of sensor technologies. Responders need small, affordable and accurate sensors.
- Subject matter experts stated that current technologies impose trade-offs in reaching the goal of geolocation to within one to three feet. Experts estimated that devices built to meet this parameter could be very expensive (tens of thousands of dollars per device).
- Systems that rely on inertial navigation require initialization, often achieved using GPS. However, GPS accuracy is, at best, within 10 to 15 feet (and worse near buildings). This further impedes the goal of geolocation to within one to three feet.
- Compensating for a lack of GPS access indoors and underground with accurate location technology may require a higher bandwidth than proximity location. This requires the use of more sophisticated devices than some of the radio and communications technology currently used on incident scenes.
- Insufficient bandwidth and cross-traffic interference may hinder the transmission of responder location data in real time.
- Each location system assumes different levels of infrastructure already present in the building. Some systems require Wi-Fi capabilities be present in a structure, while others assume no Wi-Fi capabilities.
- Systems must be tested against a variety of construction materials and building types to truly mimic reality. Finding a suitable environment that meets these needs may be difficult.

Outdoor Responder Geolocation

Relevance: Responders often operate outdoors across extensive geographic areas and in austere conditions. When deployed to these areas, responders are often unaware of the location of other nearby responders unless it is verbally communicated. In addition, incident commanders who are tasked with managing the response also may not know the location of the response teams in the field. Knowing the location of these responders and their proximity to threats is extremely important for outdoor incidents that span long distances, such as wildland firefighting. There have been instances where the lack of location information and communications has resulted in severe injury and death. In addition to safety benefits, incident commanders may also be able to allocate resources more effectively and monitor the progress of those in the field.

Current Capability: The military's blue force tracker systems provide an outdoor geolocation capability but are not designed or deployed for emergency responder use.

Currently, responders use hand-held radios (for example, 700/800 MHz, VHF, UHF) to verbally communicate coordinates to dispatch and other responders on-scene. Real-time responder geolocation can be done using GPS units, but they are costly and not widely deployed at the individual responder level. If used, these GPS locators are typically fixed to an apparatus such as a fire truck or police cruiser, which does not provide adequate location information for each responder on the incident scene.

Responder Goals:

- Accurate geolocation of responders to within one to three feet for x, y and z coordinates in hazardous outdoor environments and in remote areas
- Real-time and recurring transmission of responder location to incident command
- Graphic display of all responders on the incident scene
- Integrates with graphic display of on-scene hazards and threats
- Incorporates terrain and building information
- Integrates with common electronic situational awareness tools
- Location transmitters should be ruggedized, simple, transparent and users should not be able to turn them off
- Integration of transmitters into PPE or other existing equipment with minimal or no net weight gain for the responder
- SWP suitable for responder operating conditions
- Incorporates a confidence level to indicate the accuracy of location
- Affordable to outfit entire workforce
- Caches data when connectivity is offline, and automatically forwards when connection is restored

State of Technology: Numerous locator devices exist for markets such as outdoor recreation. For example, hikers often use personal locator beacons (PLBs) that can send out a geolocated distress signal. PLBs communicate via military satellites on a recognized distress frequency. PLBs that rely on GPS can guide searchers to within 100 meters of the user's position.[24] Other devices, called satellite transmitters, can transmit GPS location and data messages to an e-mail, cellphone short message service (SMS) or emergency response center with a pre-scripted message to convey that assistance is needed or that the user is okay. These devices only operate with a clear view of the sky and without interference from other RF signals. Therefore, being in close proximity to other GPS devices can decrease accuracy. The concern is that many of the commercial systems are not ruggedized to the response environment, do not transmit a

[24] "PLBs and Satellite Messengers," REI, last updated: n.d., http://www.rei.com/learn/expert-advice/personal-locator-beacons.html.

location continuously or in real time and cannot be networked together to provide an integrated picture of responders on scene.

DARPA has a project to help address the issue of RF interference called Advanced RF Mapping (RadioMap). This effort provides real-time awareness of radio spectrum use across frequency, geography and time. The goal is to provide a map that gives an accurate picture of spectrum use in complex environments.[25] RadioMap allows individuals to identify when the spectrum is jammed or clear, thus adding to the confidence level of how accurate a location is.

As mentioned above ("Indoor Responder Geolocation"), DARPA is also working on a geolocation program called ANS, which establishes GPS information irrespective of the operating environment.[26] Specifically, DARPA is working to develop improved IMUs, alternate sources to GPS for external position fixes and new algorithms and architectures for rapidly reconfiguring a navigation system with new and nontraditional sensors.[27]

Potential Challenges:

- Responders are concerned about the cost of outfitting an entire response unit with GPS devices and sensors that are not precise enough to improve responder safety during rescue missions.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Maritime (Above and Below Water) Geolocation

Relevance: Responders often operate in maritime environments with limited knowledge of the location of responders either on or below the surface. Having the capability to remotely monitor the location of responders, including divers beneath the surface, will improve safety and responder tactics during swift-water rescues or incidents involving maritime conveyances. Responders need the ability to know the geolocation of responders in three dimensions in maritime conditions in fresh and salt water.

Current Capability: Few technologies exist to geolocate emergency responders in the maritime environment. For geolocation on the water, GPS devices are fixed to an apparatus (for example, a rescue vessel) and not the individual responders. Therefore, incident commanders do not have a precise location of all responders at the incident scene. Most agencies do not have the capability to conduct underwater geolocation of

[25] "Advanced RF Mapping," DARPA: Strategic Technology Office, last updated: n.d., http://www.darpa.mil/Our_Work/STO/Programs/Advanced_RF_Mapping_(Radio_Map).aspx.

[26] "Adaptable Navigation Systems," DARPA: Strategic Technology Office, last updated: n.d., http://www.darpa.mil/Our_Work/STO/Programs/Adaptable_Navigation_Systems_(ANS).aspx.

[27] Ibid.

responders. Sophisticated dive teams may utilize fiber-optic umbilical cord cables tethered to a diver for location, underwater communication and safety purposes.

Responder Goals:

- Accurate geolocation of responders within three feet for x, y and z coordinates in hazardous outdoor environments and in remote areas
- Real-time and recurring transmission of responder location to incident command
- Graphic display of all responders
- Integrates with graphic display of on-scene hazards and threats
- Incorporates information pertaining to the body of water
- Integrates with common electronic situational awareness tools
- Location transmitters should be ruggedized, simple, transparent, and users should not be able to turn them off
- Integration of transmitters into PPE or other existing equipment with minimal or no net weight gain for the responder
- SWP suitable for responder operating conditions
- Incorporates a confidence level to indicate the accuracy of location
- Affordable to outfit entire workforce
- Caches data when connectivity is offline and automatically forwards when connection is restored

State of Technology: Technology for maritime geolocation is primarily focused on emergency position indicating radio beacons (EPIRBs) and personal automatic identification systems (AISs). EPIRBs work in the same manner as the PLBs described in the RTO above. The beacon broadcasts a distress signal and location coordinates via satellite. The satellite can determine the user's position to within three miles.[28] An AIS is used for tracking marine vessels. The system uses an indigenous navigation system to identify the location and speed of the vessels. Both EPIRBs and AISs are attached to the vessel, not to individuals on the vessel. Personal AIS beacons that will notify the vessel if the user is in distress have been developed for divers and boaters. The beacons use a combination of AIS and GPS signals to transmit location information but must be turned on manually. Personal AIS beacons can work at depths up to 60 meters.

[28] "What is an EPIRB?.," last updated: n.d., http://www.epirb.com/how_does_an_EPIRB_work.php.

Potential Challenges:

- Locating responders or victims underwater does not necessarily mean that the remains can be retrieved, especially if the depth or hazards in the water impede rescue efforts.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Infrastructure Standards for Technology Integration

Relevance: There are multiple opportunities for responders to leverage the information technology, surveillance and power infrastructure in buildings on an incident scene. Responders desire improved situational awareness with regard to building layouts, elevator shaft locations, structural properties and any other characteristics that may impact their response (for example, enhance or degrade communications). The collection and consolidation of this data would benefit the development of responder indoor location and communication technologies. Being able to leverage the infrastructure (for example, cameras, antennas, electrical systems) inside a building during an incident could help improve signal strength and bandwidth issues for improved indoor geolocation.

In addition to technology integration benefits, construction standards such as backup generators, pressurized stairwells, hardened elevator shafts and centralized hose plug-ins for gross decontamination efforts could improve resilience to natural and man-made events.

Current Capability: There is currently no standard for infrastructure mapping of new or existing buildings in cities across the country. Specifically, there is not a standard requiring building construction to include technology (such as radio frequency identification [RFID] tags) that would facilitate the use of responder locating devices inside structures. The International Building Code (IBC), developed by the International Code Council, addresses the inclusion of fire prevention measures during building and construction. The National Fire Protection Association (NFPA) developed an alternate code, NFPA 5000 Building Construction and Safety Code.[29] These general codes are adopted and amended by state and local jurisdictions. Revisions to these codes could include guidance on the integration of technology elements into newly constructed buildings.

[29] "NFPA 5000 Building Construction and Safety Code," National Fire Protection Association, last updated: n.d., http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=5000.

Responder Goals:

- Building code requiring:
  - Two-way communications systems for newly constructed buildings
  - Bi-directional antennas and repeaters for high rises and tunnels
  - One-way paging or intercom system to communicate with each room in the building
  - Responder access to camera systems
  - Secondary generators for sustained power loss
  - Integration of networked sensors to detect the structural integrity of the building
- Requirements to submit digital copies of all building blueprints for integration into situational awareness systems

State of Technology: The next steps for achieving responder location, rather than proximity, are dependent on the integration of multiple existing pieces of technology rather than new development. This includes installing light infrastructure (such as time-of-flight beacons and anchor sensors) in buildings before incidents occur, using LTE networks instead of radio networks, and integrating preexisting maps and building specifications into the location system. Each of these technological devices or data would greatly enhance the ability to locate a responder indoors within a narrow radius. Integrating these items would also cut down on the size and expense of any final location device, particularly the inclusion of light infrastructure in buildings before an incident. Without the light infrastructure system, sensors have to be bigger, stronger and, by extension, more expensive.

Potential Challenges:

- The addition of technology into building design will result in higher costs during construction. The building industry fought strongly against the home sprinkler requirement, and it is anticipated that it will oppose other proposed standards that increase costs.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

- There is a question of who will maintain digital copies of all building plans. The agencies responsible for maintaining residential and commercial building plans may not have systems that integrate with response agencies.

Rapid Building Characterization, Generation and Display

Relevance: Responders often arrive at an incident scene with limited knowledge of building layouts and information. Only those with extensive experience of a geographic area may be familiar with building characteristics. Responders would benefit from knowing the location of doors, exits, stairwells, power and technology infrastructure and known hazards in the building (for example, gas lines). Better understanding of building layouts would provide a significant advantage when trying to rescue a trapped or unresponsive responder as well as during other tactical operations. Responder positioning could be notably enhanced if combined with a 3-D rendering of buildings on the incident scene. Being able to quickly understand the building layout in a readily available format and the location of responders within the building can greatly improve tactical operations and decision-making.

Current Capability: Responders use open-source imagery to gain insight about target buildings. Images are typically limited to external visualizations of a building and do not provide indoor mapping capability. Digitized building blueprints are not readily available in most jurisdictions. Available blueprints have not been collected or integrated into a usable format that is accessible to responders.

Responder Requirements:

- Rapid 3-D rendering of interior and exterior features
- Readily accessible blueprints of buildings
- Includes attribute data of buildings (including the number of rooms or estimated residents living in apartment building)
- User-friendly display of information (for example, heads-up display)

State of Technology: Several technologies exist that can rapidly characterize, generate and display a 3-D visualization of a building. These technologies are not automated and require human interaction.

Multiple software platforms allow a user to rapidly create a two- or three-dimensional model of individual buildings and populate the model with known data about the building. For example, upon arrival at an incident scene, a user could identify the impacted building on a map and build a model of that building based on in-person observations such as shape, number of stories and building material type. These tools use available street-level and overhead satellite imagery as inputs for the creation of the models. Integrating up-to-date maps and preexisting building data can help improve the technology's output and provide greater detail for the response community.

These 3-D renderings can be integrated into other software programs that illustrate incident effects. The Defense Threat Reduction Agency (DTRA) funded the development of NucFast, a software platform that uses National Geospatial-Intelligence Agency (NGA) building footprint data to model the 3-D structural components of buildings. The system incorporates data sets from the Federal Emergency Management Agency's (FEMA) Hazus program to model the effects of a nuclear detonation. The system can display a range of effects (for example, rubble pile distribution, thermal loads, structural failures, probability of fire initiation) at the individual building level. The outputs of this system could be used to significantly improve the safety of responders and the population.

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

- Many existing building plans are not digitized and it may require a significant effort to convert existing files.
- Digital building plans will need to be updated as buildings and structures are renovated. Responders need access to the most recent copy of the plans. However, there is a question (as mentioned above) regarding which agency is responsible for obtaining and maintaining these updated plans in each municipality.
- Responders noted that there may be privacy challenges related to estimating the number of residents living in apartment buildings or multi-family dwellings.

Improved Standoff Detection and Identification of Multiple Hazards

Relevance: Responders face a large number of diverse hazards during a catastrophic incident, including caustic gases and volatile organic compounds (VOCs), radioactive contamination, biological agents, deficient oxygen levels and explosives and secondary devices. These hazards can be detected, characterized and measured using sensor technology. Specifically, sensors that measure the quantity, volume and concentration of these hazards provide the basis for making time-sensitive decisions that impact the health of responders and the public. This RTO focuses on the initial detection of hazardous agents and characterization of critical information. Ongoing surveillance and monitoring of threats is covered in a separate RTO called "Remote Monitoring of Threats and Hazards."

Current Capability: Responders currently use a variety of sensors and detectors to detect hazardous agents, including personal radiation detectors (PRDs), multi-gas chemical detectors, infrared sensors, medical infection control sensors and motion detectors. However, accessibility to and availability of these devices varies depending on jurisdiction. For example, all New York City responders (law enforcement, fire and EMS) carry PRDs, but only district-level law enforcement supervisors in other jurisdictions carry these devices. Cost is one of the most prohibitive factors impacting availability. Additionally, the spectral range for available devices is limited. For example, the majority of PRDs detect gamma signatures but do not have the ability to identify individual isotopes or neutrons. Conversely, chemical sensors can identify a specific agent but cannot provide concentration levels from a safe distance. Responders reported that they have no sensor or detector for real-time biological agent detection or identification. Most of the current detectors and sensors can be mounted to various platforms, including manned and unmanned ground vehicles and aircraft. Other technologies utilized for this capability include building security systems, acoustic sensors and multi-spectral cameras.

Resources such as the Radiation Emergency Medical Management (REMM) tool and the *Emergency Response Guidebook* (ERG) provide a consolidated repository of approved information and aid in the characterization of hazards. These resources provide guidance about radiological and chemical incidents, including information about individual isotopes or toxins, standoff distances, relevant protective actions and basic medical treatments or countermeasures.

Responder Goals:

- Detects hazardous agents in real time, including chemical, biological, radiological and explosive particles and signatures, within a set perimeter around response personnel
- Identifies the specific agent or isotope
- Detects or measures other pertinent data (for example, oxygen displacement) that impacts hazardous conditions
- Measures the current concentration and records exposure over time
- Provides pertinent information, including modes of exposure, protective action information (for example, appropriate PPE, standoff distances, immediate treatments, decontamination requirements)
- Generates automated alerts in multiple formats (in other words, audible, visible, tactile) when preset or site-specific thresholds have been reached
- Integrates personal detectors into PPE, communications devices or other daily equipment
- Affordable to outfit entire workforce
- Relays information in real time to incident command, caches data when connectivity is offline, and automatically forwards when connection is restored
- Integrates with common electronic situational awareness tools
- Deployable on multiple platforms (for example, manned and unmanned ground and aerial vehicles, fixed and mobile)
- Compliant with relevant standards
- Equipment should be intrinsically safe and ruggedized

State of Technology: There are multiple technologies in development that could improve capabilities for identifying and characterizing hazards on the incident scene.

A commercial manufacturer developed a chemical detection armband that uses a customizable set of chemical detector cassettes. The system uses a color-changing detection system that alerts the user to the presence of a toxic gas. The U.S. Coast Guard uses the system extensively. The company developed preconfigured kits for hazardous materials (hazmat), clandestine methamphetamine labs and other specific incidents to expand use to the response community.

Other applications are being developed specifically for the response community. S&T recently developed Chem-Tag, a small, lightweight, low-cost unit that alerts users when it detects carbon monoxide, methane or hydrogen cyanide.[30] S&T anticipates that Chem-Tag could be integrated into responder garments or equipment. A related program, in development by S&T's Homeland Security Advanced Research Projects Agency (HSARPA), is the Cell-All sensor, designed to continuously "sniff" the air around the user for volatile chemical compounds.[31] S&T envisions that it will be integrated into publicly available smartphones, providing alerts to individual citizens when it detects that they are in the presence of hazardous chemicals and alerting authorities after identifying specific threats such as chemical warfare agents. Similar technologies use a smartphone's camera to detect radioactivity. The current version of the system allows users to monitor personal radiation exposure, but it is anticipated that users will soon be able to compare their measurements with others in their area. Radiation measurements can also be transmitted to response personnel.

The DHS Domestic Nuclear Detection Office (DNDO) is developing technologies for spectroscopic personal radiation detectors that can better detect, identify and locate radiological or nuclear sources. The devices use advanced scintillating materials, which help to better identify specific sources than can be done with current materials.[32] DNDO is also supporting the development of domestic capability to produce stilbene, an organic scintillator for the passive detection of neutrons.[33]

DARPA leads many of the advances in this area and is primarily focused on addressing deficiencies in current systems. For example, DARPA has funded a program called the Compact Mid-Ultraviolet Technology (CMUVT) program.[34] The goal of this program is to develop ultraviolet (UV) components that will improve the size, weight, power and capability of chemical- and biological-agent detectors. Another DARPA program, the Advanced Wide FOV Architectures for Image Reconstruction and Exploitation (AWARE), is using innovative camera designs and distributed aperture sensors to create a gigapixel camera small enough to be deployed on a small unmanned aerial platform.[35]

[30] "Smartphones now capable of detecting gas," Homeland Security News Wire, October 3, 2011, http://www.homelandsecuritynewswire.com/node/33274.

[31] "Cell-All: Super Smartphones Sniff Out Suspicious Substances," DHS, last updated: December 26, 2012, http://www.dhs.gov/cell-all-super-smartphones-sniff-out-suspicious-substances.

[32] "Advanced Radiation Monitoring Device," DHS, last updated December 31, 2013, http://www.dhs.gov/advanced-radiation-monitoring-device.

[33] "Stilbene, an Organic Scintillator for Fast Neutron Detection," DHS, last updated June 16, 2014, http://www.dhs.gov/stilbene-organic-scintillator-fast-neutron-detection.

[34] "Compact Mid-Ultraviolet Technology," DARPA: Microsystems Technology Office, last updated: n.d., http://www.darpa.mil/Our_Work/MTO/Programs/Compact_Mid-Ultraviolet_Technology_(CMUVT).aspx.

[35] "Advanced Wide FOV Architectures for Image Reconstruction and Exploitation (AWARE)," DARPA: Microsystems Technology Office, last updated: n.d, http://www.darpa.mil/Our_Work/MTO/Programs/Advanced_Wide_FOV_Architectures_for_Image_Reconstruction_and_Exploitation_(AWARE).aspx. The acronym FOV in the title refers to field of view.

Real-time detection of biological agents remains a challenging problem. DHS S&T funded the Detect-to-Protect (D2P) program to assess multiple sensors that have been designed to identify and confirm the release of biological agents within minutes. The D2P program held a series of tests in 2012 to detect biological agents in the Boston subway system.[36]

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

- Responders did not specify a precise desired standoff distance. Subject matter experts stated that this is a critical point as the size, weight and cost of the sensor rise, and performance degrades, as the distance is extended.
- Responders are continuously concerned about false positives and negative rates, which in turn could lead to distrust and disuse of technology.
- Similarly, there are concerns about false positives and inaccuracies from cellphone applications that detect radiological signatures. The public may not have sufficient understanding of the measurements, other potential sources of radiation (for example, nearby persons receiving nuclear medicine treatments) or the effects of background radiation to properly assess and understand alerts from these applications.
- The accuracy of sensor systems is increased when the measurements are analyzed against normal background levels for agents and contaminants. However, few communities collect such data.

Multi-sensor Integration and Analysis

Relevance: Responders need to be able to assess their current level of risk from multiple threats. For individual responders, this generally involves carrying multiple types of sensors on their person as part of their PPE, in their hands, or deployed on an apparatus (for example, radiation pagers, five-gas meters). Incident command also relies on measurements from multiple types of fixed and mobile sensors deployed on numerous platforms. However, the measurements and readings from these sensors are rarely integrated, and analysis of the results is done individually. This RTO focuses on the integration and miniaturization of sensors so they can be deployed on a smaller number of platforms and the analysis of those sensors can be combined to provide a comprehensive picture of hazards on the incident scene.

[36] "DHS using Boston subway system to test new sensors for biological agents Homeland Security News Wire," *Homeland Security Newswire*, August 27, 2012, http://www.homelandsecuritynewswire.com/dr20120827-dhs-using-boston-subway-system-to-test-new-sensors-for-biological-agents.

Current Capability: There is limited integration of sensors and analysis conducted in the response community. The primary exception is the multi-gas meter, which is a single system that can identify oxygen levels, lower explosive limits (LELs) and concentrations of the most common VOCs (for example, ammonia, chlorine, hydrogen cyanide, phosphine, and sulfur dioxide). Advanced models include radiation detection and the ability to interchange toxic sensors. These are available in hand-held devices or larger, mobile devices that allow standoff detection and monitoring of hazardous agents.

Responder Goals:

- Appropriate SWP for integration of multiple sensors and imaging systems into several platforms, including:
    - Personal device (size and weight of a deck of cards)
    - Man-portable systems (backpack size, less than 25 pounds)
    - Unmanned aerial systems (under six pounds)
    - Unmanned ground vehicles (weight unspecified)
- Includes a common hub or interface, allowing interchangeable sensor configuration
- Ability to adjust or tune sensors for different environments (for example, smoke, steam)
- Ability to network sensors and integrate outputs and data measurements for combined assessment of existing hazards
- Integrates with common electronic situational awareness tools
- Relays information in real time to incident command, caches data when connectivity is offline and automatically forwards when connection is restored

State of Technology: Subject matter experts advised that nanotechnology might offer substantial enhancements in the development of new and smaller sensors. Scientists from the Center for Nanotechnology at the National Aeronautics and Space Administration (NASA) Ames Research Center developed a chemical-sensing, platform-based nanotechnology.[37] Each sensor in the array consists of a nanostructure, chosen from many different categories of sensing material that can measure the concentration of chemical molecules. Researchers believe that lightweight and compact sensors can be made at low cost.

DARPA is also investing in miniaturized sensors. One example is the Low Cost Thermal Imager-Manufacturing (LCTI-M) program.[38] Researchers are trying to develop very low-cost, high-performance thermal imagers that can be can be inserted into hand-held units,

[37] "Carbon Nanotube Sensors for Gas Detection," NASA, last updated: March 29, 2008, http://www.nasa.gov/centers/ames/research/technology-onepagers/gas_detection.html.

[38] "Low Cost Thermal Imager-Manufacturing," DARPA: Microsystems Technology Office, last updated: n.d.,http://www.darpa.mil/Our_Work/MTO/Programs/Low_Cost_Thermal_Imager_(LCTI-M).aspx.

modified cellphone products, rifle sights, helmets, eyeglasses, micro-Unmanned Aerial Vehicles (UAVs) and other small form-factor devices for real-time target recognition, acquisition and network sharing of data. The goal is for the devices to be made available for every vehicle, surveillance device and dismounted warfighter, significantly improving situational awareness.

HSSAI research found few ongoing efforts to develop a standardized plug or hub for the integration of sensors onto a common platform. The chemical armband described in the RTO above represents one success in this area. The system includes 14 different sensors that can be interchanged on the armband to create a configuration that best meets the needs of the user. The sensors are packaged in cassettes that plug into the armband base. The form factor for each cassette is the same, allowing it to take any place on the base. While integrated onto the same armband, the sensors are not fused together to give an integrated indication of hazards. Other manufacturers have developed bridging devices with multiple connectors attached via wires to a central hub. Such devices allow sensors from different manufacturers to be used on the same platform. One issue is that there are limited connectors of any one type, restricting the number of sensors from the same manufacturer that can be attached.

Potential Challenges:

- Participants stated that manufacturers might be unwilling to use a standard hub or plug configuration for their sensors, citing commercial advantages in having proprietary interfaces.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

Risk Assessment and Decision Support to Command

Relevance: The sensors and imaging systems involved in the identification, characterization and monitoring of threats and hazards may produce large amounts of technical data and require analysis of complex information. These data include sensor readings, model projections, reporting of conditions from the incident scene and other pertinent information. In many cases, command staff members cannot incorporate the large amounts of data coming in or do not have the technical training to understand the data and information. This makes it difficult for incident command to assess the level of risk and make appropriate life-safety or operational decisions. Responders stated the need for a decision support system that will improve their understanding of the threats and hazards on the incident scene and support accurate decision-making. This RTO is important because increased understanding of pertinent data and information will allow command staff at all levels to make decisions that improve responder and population safety.

Current Capability: There is no single source of information that incident command can use to make key decisions about hazards and threats. Information is available in multiple sources and formats, but it is not integrated with a tool that guides incident command staff through response.

Responder Goals:

- Guides incident command staff through key decisions points, integrating actual and projected data and information (including sensor readings, model outputs, technical calculations, first-hand accounts from the scene, etc.)
- Provides recommended decisions or courses of action for each decision point and confidence levels for those recommendations
- Indicates where key inputs are missing that could improve confidence levels
- Provides cues and checklists for additional support
- Integrates all risk alerts onto one common display
- Integrates with common electronic situational awareness tools
- Incorporates the criteria levels (for example, established exposure limits) established during pre-planning efforts
- Includes pre-populated and user-defined decision points

State of Technology: Several decision support systems are commercially available to the emergency response community. These systems integrate incident-specific measurements with modeling capability to provide specific operational recommendations and guidance. One example is the Chemical Companion Decision Support System, funded in part by the Technical Support Working Group (TSWG) and the U.S. Marine Corps Systems Command.[39,40] The software is accessible via mobile devices and desktop and laptop computers. The chemical companion offers decision support capability, such as a respiratory protection tool that guides users through a series of questions about environmental conditions and hazardous materials and delivers a recommendation on what type of respiratory protection is required. A detection tool helps the user determine which detectors should be used and aggregates the results of multiple devices. The chemical companion is free to law enforcement and fire departments.

Decision-makers face challenges in rapidly evolving environments when there may be a lack of communication or situational awareness. In an attempt to overcome these

[39] The Technical Support Working Group conducts the national interagency R&D program for combating terrorism through rapid research, development, and prototyping. "Our Missions," Combating Terrorism Technical Support Office, last updated: n.d., http://www.tswg.gov/?q=missions.

[40] "Chemical Companion Evolves from Information Resource to Sophisticated Decision-Support System," Georgia Institute of Technology, last updated February 19, 2014, http://www.news.gatech.edu/2014/02/19/chemical-companion-evolves-information-resource-sophisticated-decision-support-system.

challenges, DARPA established the Distributed Battle Management (DBM) program.[41] The goal of this program is to develop automated decision aids to assist airborne battle managers and pilots with managing air-to-air and air-to-ground combat. While this particular application is DOD-specific, the research and conceptual application of automated decision aids could also have applications for the civilian response community.

Potential Challenges:

- Responders may be hesitant to rely on computer-generated recommendations.
- Participants stated that liability concerns might hinder development of this system. Developers will not want to expose themselves to criminal or civil liability if the guidance is inaccurate or inconclusive.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

Remote Monitoring of Threats and Hazards

Relevance: It is important for emergency responders to have the ability to continuously evaluate existing, emerging and potential hazards in areas affected by a catastrophic incident. Areas that may need monitoring include a broad radius around an incident scene, areas where response and recovery actions are underway or specific ingress/egress routes. Remote monitoring provides the necessary input for incident command to assess the present dangers and emerging threats over time without exposing responders to additional risk. This RTO focuses on the development of multiple platforms to support monitoring of threats and hazards on the incident scene and potentially affected areas. This RTO is important because real-time, continuous surveillance improves the safety of emergency responders and the affected population still in those defined areas. This RTO focuses on the ongoing surveillance and monitoring of threats through the development of multiple platforms. Initial detection and characterization of hazardous agents is covered in a separate RTO (see "Improved Standoff Detection and Identification of Multiple Hazards").

Current Capability: Responders currently rely on several fixed and mobile platforms for remote monitoring of the incident scene. In many cases, man-portable systems are placed throughout the incident scene and affected area, but this involves risks to the personnel placing the system. Sensor systems are also often attached to manned aircraft to provide aerial images and measurements. Responders also rely on traffic and surveillance cameras to remotely monitor key areas. In addition, some Special Weapons and Tactics (SWAT) teams use unmanned ground vehicles (UGVs) for remote assessment of threats (primarily explosive devices), but these are cost-prohibitive for many agencies.

[41] "Distributed Battle Management," DARPA: Strategic Technology Office, last updated: n.d., http://www.darpa.mil/Our_Work/STO/Programs/Distributed_Battle_Management_(DBM).aspx.

The Federal Aviation Administration (FAA) currently prohibits the use of most unmanned aerial systems (UAS) for response operations, but they are used to a limited extent.[42] In addition, many states have enacted laws prohibiting or significantly limiting the use of UAS by law enforcement.

Responder Goals:

- Platforms to remotely capture threat- and hazard-related data in multiple topographies (for example, inside buildings, at various depths and elevations, over rubble and across different terrains)
- Operates within multiple environments (for example, smoke, humidity)
- Equipped with configurable sensor packages (see the "Multi-Sensor Integration and Analysis" RTO)
- Platforms in various sizes and configurations (for example, UGVs, UAVs, mobile and man-portable systems)
- Uses a common hub or interface for sensors and imagers
- Continuously integrates captured data with geographic information system (GIS) location of platform
- Able to operate multiple platforms in networked and/or swarm configuration
- Equipment is ruggedized, intrinsically safe and nondegradable due to hazard
- Sufficient power supply to support duration of monitoring (variable by platform)

State of Technology: Unmanned aerial and ground systems are well suited to carry sensors that detect threats and hazards. Use of these systems for emergency response is currently limited by government restrictions, liability concerns and cost.

UAS technology is mature, and the platforms are used regularly by DOD in its operations outside of the United States to conduct many of the same tasks that emergency responders would perform. The systems can provide sustainable monitoring of threat and hazard conditions over the incident scene and affected areas and regularly carry traditional remote sensing payloads, such as hazard sensors or multispectral cameras.

Advances in UAS may provide significant improvements in capability once regulatory issues are resolved. UAS that can be used for domestic missions range in size from the large Predator (27 feet long, 2,250 pounds loaded and unit cost of approximately $4 million) to hand-launched platforms that weigh less than 10 pounds. DHS S&T is currently funding the Robotic Aircraft for Public Safety (RAPS) project to test and evaluate Small Unmanned Aircraft Systems (SUAS) equipped with sensors, including various imaging systems.

[42] The term *unmanned aerial vehicle* has largely been replaced with the term *unmanned aerial system* to reflect the fact that the vehicles are complex systems controlled by human operators.

Small unmanned ground vehicles (also referred to as robots) are able to enter buildings and other structures that may be inaccessible for aerial systems. Advanced robots are able to climb stairs, open doors and move over uneven terrain, including rubble. The BigDog robot, funded by DARPA, can transport heavy loads of remote sensing payloads over terrain that cannot be traversed by wheeled or tracked UGVs.[43] There are ongoing DARPA efforts to improve the bullet resistance of BigDog, which could allow it to operate during an active shooter incident. Other developers are focused on using microrobotics to create small platforms (some only a centimeter across) that can be deployed to reach small areas or confined spaces.

Robots are regulated by Occupational Safety and Health Administration (OSHA) requirements, which ensure that their electronics will not ignite fuel or cause an explosion (referred to as intrinsically safe). Subject matter experts stated that complying with these requirements adds significantly to the cost of the platform, making the price unreachable for many response agencies.

Developers are also working to reduce the costs of UAVs and UGVs through the application of 3-D printing for on-site manufacturing of platform components. Agencies will be able to rapidly print the non-electrical parts of these platforms to build low-cost parts. Printable components include wheels, cases, wings and braces. Developers envision a "kit in a box" option that would enable users to purchase a set of electronic components and print the other required pieces for the UAV or UGV. Parts can be printed on-scene with commercially available 3-D printers (which are becoming less expensive and more accessible for response agencies).[44]

Potential Challenges:

- Federal and state regulations and restrictions hinder the application of UASs for emergency response missions within the National Airspace System.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

Combined Effects Assessment

Relevance: Large-scale incidents typically present multiple threats and hazards to emergency responders. The initial hazard often causes secondary or cascading effects, each presenting a unique challenge for responders and presenting unforeseen risks to both responders and the public. The tsunami that hit Japan in 2011 illustrates the potential for multiple and combined effects. This natural disaster caused radiological and chemical

[43] "BigDog – The Most Advanced Rough-Terrain Robot on Earth," Boston Dynamics, last updated: n.d., http://www.bostondynamics.com/robot_bigdog.html.

[44] On-site 3-D printing has additional applications for emergency response outside of UAV or UGV platforms. Responders will be able to print spare or replacement parts for multiple pieces of equipment on scene.

incidents, numerous fires and the collapse of a dam.[45] Incident command needs to understand the potential for secondary effects, the conceivable impacts of all incident effects and how those effects combine to mitigate or exacerbate the situation. This information will allow incident command to assess the priorities of threats and make appropriate PPE and protective decisions for responders and the public. Responders want to address the most critical impacts without ignoring the potential for secondary issues or consequences.

Current Capability: There is little integrated capability to understand and assess combined incident effects. In many cases, jurisdictions identify potential hazards and potential effects through pre-event assessments, but do not include incident-specific information based on actual conditions. There are several tools available for characterizing hazards during an incident, including the Hazard Prediction and Assessment Capability (HPAC), Computer-Aided Management of Emergency Operations (CAMEO), and HotSpot. These tools can be used for both pre-event planning and post-incident overlay of data to indicate hazards. In addition, many tools use GIS overlays that allow "painting" of hazards on a map of the incident scene.

Responder Goals:

- A multi-layer graphic display that illustrates individual and combined hazards on a GIS-enabled street-level map, including critical infrastructure and key resources (CIKR) and known hazards
- Calculates combined effects supported by sensor measurements and model outputs
- Integrates outputs with digital situational awareness tools
- Includes decision support materials to prompt consideration and analysis of potential secondary effects
- Includes predictive modeling functionality to illustrate the impacts of potential secondary or combined effects

State of Technology: Advances in technology for this RTO are primarily focused on the graphic display of threats and hazards for improved situational awareness. The Idaho National Laboratory, for example, is developing a robotics platform that will both map the interior of a structure and display the presence of chemical or radiological hazards on the map. The system uses lasers to create a two- or three-dimensional map of the building infrastructure, and the presence of each hazard is illustrated through a series of colored

[45] On March 11, 2011, an undersea earthquake triggered a tsunami that caused extensive damage, resulting in nearly 25,000 casualties and damage to more than one million structures. The tsunami also caused a nuclear accident at the Fukushima Daiichi nuclear plant after seawater flooded the rooms where emergency generators were stored, diminishing power available for the coolant system. Lack of electrical or backup power sources led to a meltdown in three of the seven reactors. Chemical explosions occurred in two of the reactors at Fukushima due to high concentrations of hydrogen gas. The tsunami also caused a separate, large explosion at a petrochemical plant.

layers. This system would potentially allow responders to avoid hazardous areas when conducting operations inside of structures. The robotics platform could also carry a camera, allowing responders to see images of threats or hazards before they enter.

A number of other systems have been developed to display multiple threats on GPS maps, helping to create a common operational picture of the threats and hazards present on the incident scene. These systems allow the user to import digital images of the incident scene, many of which are readily available on the Internet. The user builds shapeforms onto the image and customizes a graphic display of buildings and structures on the incident scene. The user can then overlay threat and hazard data and other information onto the 3-D map, including plume models and images. Advanced systems incorporate additional modeling capability, such as rubble pile distribution, thermal loads on infrastructure, structural failures and air-blast effects.

Potential Challenges:

- Despite advances in graphic display of threats and hazards, there are deficiencies in the ability to assess the impact of threats and hazards on each other and the resulting impacts on response operations and responder health.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

- Building and customizing shapeforms to create a 3-D display of the incident scene is not complex, but does take time (depending on the size of the incident scene). The utility of existing systems would be significantly improved if communities develop 3-D image files of structures before an event.

Automated Red-force Tracking

Relevance: In the military realm, hostile or opposing forces are referred to as "red forces" and friendly forces are referred to as "blue forces." The emergency response community uses a similar concept. Red forces denote a specific threat or hazard and could be a person or persons (for example, active shooters, suspects) or an item such as a weapon or an explosive device. In a hostile situation, responders and decision-makers need to know the location and movement of these threats and their proximity to other response personnel, critical resources and infrastructure. Real-time tracking of red forces can allow incident command to improve the safety of response personnel and enable more efficient neutralization of the threat.

Current Capability: On an incident scene where there are red forces such as active shooters, it is critical for responders to have situational awareness and know the location of the threats. Responders do not currently have an integrated red-force tracking technology platform. Instead, they utilize a host of tools, including closed-circuit television (CCTV) and other video cameras, social media, visual surveillance and facial recognition software to identify and track threats. Red-force tracking technology is used to identify and monitor the movements of enemy forces on the battlefield, but these technologies have not been adapted for domestic use.

Responder Goals:

- Integrates with responder location/tracking system
- Identifies red-force elements
- Generates covert alerts to responder regarding proximity to red force
- Integrates red-force tracking into situational awareness tools for tactical decision support
- Identifies when a red force approaches high-risk areas/targets
- Ability to covertly place surveillance tags on a red force
- Displays data in heads-up field of view

State of Technology: The U.S. military funds a number of development efforts to identify and track threats. Primarily designed for blue-force tracking, several systems allow warfighters to visualize friendly and hostile forces on a graphic display.

The U.S. Army's Force XXI Battle Command Brigade-and-Below/Blue Force Tracking (FBCB2/BFT) provides advanced situational awareness to warfighters.[46] Warfighters see blue icons on a computer screen inside their vehicle, indicating the location of their teammates. They can also plot improvised explosive devices and enemy locations with red icons on the same computerized topographical map, which are visible by all team members.

A similar capability is available in helmet-mounted heads-up display (HUD) units that allow users to identify and tag persons thought to be a threat. The tagged persons are shown with an icon that is continuously visible in the field of view, even if the threat is not. The system is able to calculate and display the distance of the warfighter from the identified threats.

DARPA is funding the Urban Leader Tactical Response, Awareness and Visualization (ULTRA-Vis) program, which is focused on creating a prototype for an augmented reality system.[47] Augmented reality is accomplished by superimposing a computer-generated image onto the user's view of the real world. This should allow warfighters to overlay full-color graphical iconography onto the local scene as observed by the soldier. The augmented reality system is a lightweight, low-power holographic see-through display

[46] "Army fields next-generation blue force tracking system," U.S. Army, last updated July 15, 2011, http://www.army.mil/article/61624/.

[47] "Urban Leader Tactical Response, Awareness and Visualization," DARPA: Information Innovation Office, last upated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/Urban_Leader_Tactical_Response,_Awareness,__Visualization_(ULTRA-VIS).aspx.

with a vision-enabled position and orientation tracking system that the warfighter wears. In doing so, warfighters are able to significantly increase their understanding of the areas and visualization of threats.

DARPA is also focusing on advances in imaging systems to support red-force tracking. For example, the Autonomous Real-Time Ground Ubiquitous Surveillance-Infrared (ARGUS-IR) is a 1.8 billion-pixel sensor system for persistent tracking of threats.[48] ARGUS-IR can be deployed on UAS or UGV platforms.

Potential Challenges:

- Responders reported concerns with mis-identification of threats when using a red-force tracking system. In addition to the potential for labeling friendly forces as hostile, there could be significant liabilities associated with taking actions against innocent civilians.
- Law enforcement officers currently face legal and privacy issues with using technologies such as facial recognition for red-force identification and surveillance of red-force actors.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

All-source Collection and Integration of Data

Relevance: The ability to incorporate information from multiple and nontraditional sources into incident command and operations is a well-defined need from the emergency responder communities. There has also been an increase in disaster-affected populations that utilize social media platforms to communicate and self-organize to identify needs, threats, and solutions during an incident. Emergency responders at the federal, state and local levels have voiced interest in using nontraditional sources of information to improve decision-making through increased situational awareness and public information needs. This information could take the form of crowdsourced information or social media data, for example. The response community would like to use this information in conjunction with traditional information sources (for example, sensor readings, 311 data, weather maps, traffic camera feeds) to improve decision-making during emergencies.

Current Capability: Responders are currently facing data overload. Most information coming from the incident scene is collected, analyzed and disseminated by individuals, with little help from technology. Making sense of large volumes of information can be difficult and time consuming. Some agencies use social media in limited ways, including monitoring individual tweets, posts and other content. However, they do not use high-performance analytics to rapidly make sense of large quantities of information, so they do

[48] "Autonomous Real-Time Ground Ubiquitous Surveillance – Infrared," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/Autonomous_Real-time_Ground_Ubiquitous_Surveillance_-_Infrared_(ARGUS-IR).aspx.

not gain adequate situational awareness from these sources. Overall, the capability to collect and analyze big data is limited, and the emergency response community has not developed or endorsed a standard operating procedure for collecting, analyzing and integrating social media data into operations.

Responder Goals:

- Ingests data in multiple formats (for example, keyhole markup language [KML], keyhole markup language zipped [KMZ], Javascript object notation [JSON])
- Automates the collection and display of data streams
- Identifies those individuals that the public relies on for information and/or whose messages have more influence over the actions of others
- Determines sentiment of social media messages
- Automates the classification of information and dissemination of threat information
- Ensures the security of collected information
- Integrates and overlays social media data on top of existing data sources
- Provides a customizable search function with simple queries
- Automates queries and alerts responders for anomalies or results that need to be investigated
- Conducts analysis (for example, trend and pattern, link, sentiment, keyword alerting) in real time
- Displays confidence levels to inform decision-makers of information accuracy
- Filters exigent social media content from metadata (for example, embedded exchangeable image file format [exif] data)
- Produces customized reports and visualizations in different formats for dissemination

State of Technology: There are numerous tools available to assist emergency responders with visualizing data, including platforms that allow a user to view data in different layers. State emergency management offices are also working in this area to build virtual systems that collect and display information to make it accessible for responders (for example, Virtual Alabama). Tools that mash up data can be useful, yet data collection and analysis are time consuming and largely dependent on the responder. Without the aid of technology that can automate some of the analytics to reduce cognitive load, responders may quickly get overwhelmed with the large volume of incoming data during a catastrophic incident.

A lot of progress has been made in the past few years on technologies to automatically collect, analyze and disseminate data, including that from nontraditional sources such as social media content. These tools, however, are not immediately available or ready for use by the emergency responder community. Furthermore, data from nontraditional sources (for example, audio, photo, video, sensors) has not been effectively combined, and its fusion remains a technical challenge. Emerging technologies have been used in pilot studies and ad hoc experiments, each resulting in mixed results. Many of these technologies do not easily integrate with other systems and are not "responder friendly" or able to be used in realistic operating conditions without significant assistance from developers.

To date, most existing social media and other data fusion technologies have not been developed with an emergency response application in mind. As a result, the outputs yield limited actionable information that is in formats that are not easy for the response community to quickly analyze and use to make decisions.

Similar to emergency responders, DOD systems have difficulty managing the vast amount of information intake. Therefore, DARPA started a program called XDATA to enhance the ability of software tools to process and analyze large and incomplete data sets.[49] The goal of this research is to enhance the ability to use timely and actionable information to make well-informed decisions.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

Potential Challenges:

- Building collaboration with the public and private sectors to share information and input can be challenging.
- Sharing information is often hindered more because of human barriers (for example, existence of or lack of reciprocal trust, commitment to keep information in shared databases current) than technology barriers. These issues will not be resolved through the development of new technology.
- Technology in development needs to keep up to date with evolving social media and other nontraditional source information.
- There are privacy concerns with using personally identifiable information that need to be addressed.
- There are technical challenges with the collection and integration of unstructured data not available in a standard application programming interface (API) with other data streams.

[49] "XDATA," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/XDATA.aspx.

All-source Information Validation

Relevance: There are many different situations where responders have difficulty validating information that comes in through 911 or social media, including unverified calls or reports, until a responder adjudicates the information on-scene. The ability to validate information, tips from the public or other incident-specific information is important when responding to an incident. The ability to validate information becomes harder when responders attempt to incorporate nontraditional information sources, such as social media, with traditional sources.

Current Capability: Currently, there are very limited examples where crowdsourcing or technology aids the verification process of incoming information. To date, validation of incident scene data is largely a human-based capability from responders on-scene. In industry, however, there are examples of data (for example, traffic reports) being validated through crowdsourcing. This type of third-party validation might have application in the emergency response enterprise.

Responder Goals:

- Automated validation of nontraditional information and data
- Includes confidence level indicator for how valid data might be
- Validates the user, time, and location of the information
- Validates content including text, photos, and videos
- Analyzes patterns, behavior, and history of user
- Integrates historical and environmental trends and alerts when aberrations occur

State of Technology: Technology to automatically collect, integrate and analyze data is still emerging, and so is the ability to validate that information. Currently, the state of the art for data validation relies mostly on contributions from large groups of people, called crowdsourcing.

Crowdsourcing is increasingly used by responders to gain situational awareness and validate information. For example, one mobile application uses crowdsourcing as a way to identify and confirm road status, hazards, police activity and other pieces of data to help drivers gain better situational awareness. This type of crowdsourcing is done in real time: drivers can easily plot points of interest, and other drivers nearby are asked to confirm the information. Once the data points have been confirmed multiple times, they are plotted on a map. If the data points are disputed multiple times, they are removed from the map. This creates a dynamic map of crowdsourced information that maintains itself with other users keeping it up to date.

DARPA has also incorporated crowdsourcing into a process that more effectively evaluates commercial off-the-shelf (COTS) software. This process, called the Crowd Sourced Formal Verification (CSFV) program, uses large numbers of non-experts to perform formal verification faster and more cost-effectively than the traditional approach of a few specialized engineers.[50] To accomplish this, DARPA has developed a simulation game that creates a fun and interactive environment to help complete formal verification proofs.

Other technologies exist that validate whether a post or photo has been edited or published elsewhere using a photo's exif data. This data is embedded within the image file itself and contains location information. Similar to how online image gallery programs recognize this data and can display the date and location of a photo, other tools can use this to detect false or uncertain information that is published following an event.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

Potential Challenges:

- Given the nature of crowdsourcing, it is difficult to validate certain data in real time.
- There may be issues related to gaining access to information necessary for verification.

[50] "Crowd Sourced Formal Verification," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/Crowd_Sourced_Formal_Verification_(CSFV).aspx.

Situational Awareness Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the situational awareness RTOs above.

- Continue enhancement of sensors and other technologies to improve signal strength around and through barriers
- Transition existing state-of-the-art technologies for outdoor responder geolocation
- Transition existing technologies and improve signal transmission in maritime environments
- Obtain necessary consensus to develop infrastructure and construction standards for newly constructed buildings
- Integrate responder geolocation technologies with systems for automated 3-D rendering of interior infrastructure from digital blueprints
- Continue development of detection and identification devices
- Continue development of sensor technologies, including miniaturization (to integrate with small UAS and UGVs) and modularization
- Develop standard public safety UAS platform (total weight under 55 pounds; payload weight under 6 pounds; hand-launched; low power supply; simple data transmission; standardized payload interface; under 400-foot altitude) and a low-cost standard public safety robot (standard payload interface)
- Encourage adoption of legislation that authorizes public safety use of UAS platforms
- Enhance and integrate modeling outputs to display multiple threats on a common operating platform
- Transition existing state-of-the-art technologies used for military application to emergency response use
- Identify information needs and requirements, resources and data streams for data integration
- Identify data streams that need to be validated using training set of human and historical data; develop algorithms to assess data sources for validation signatures

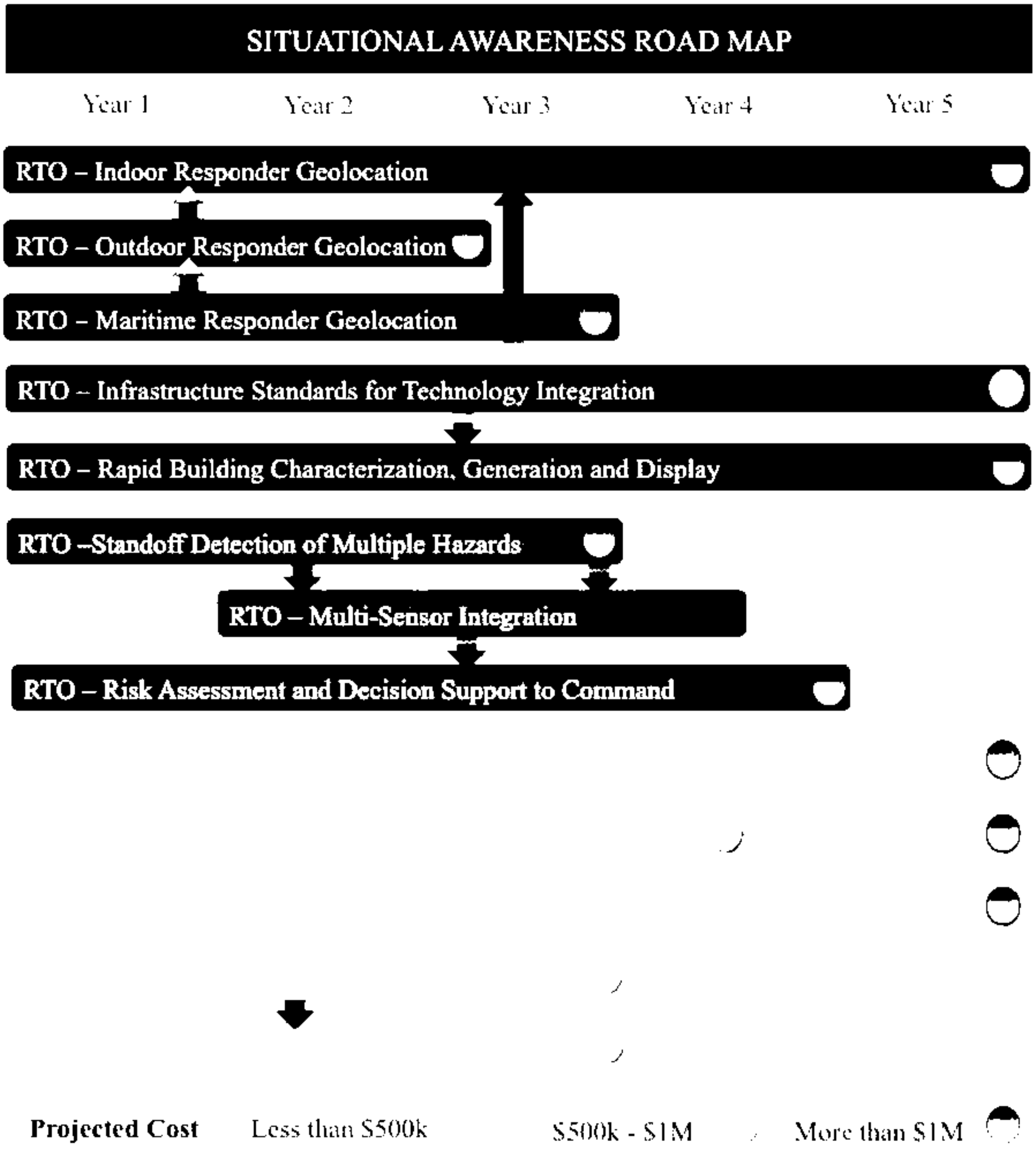

SITUATIONAL AWARENESS ROAD MAP
Year 1
Year 2
Year 3
Year 4
Year 5
RTO – Indoor Responder Geolocation
RTO – Outdoor Responder Geolocation
RTO – Maritime Responder Geolocation
RTO – Infrastructure Standards for Technology Integration
RTO – Rapid Building Characterization, Generation and Display
RTO –Standoff Detection of Multiple Hazards
RTO – Multi-Sensor Integration
RTO – Risk Assessment and Decision Support to Command
Projected Cost
Less than $500k
$500k - $1M
More than $1M

Figure 10. Situational Awareness Technology Road Map

Communications is defined as the capability to seamlessly and dynamically connect multiple persons or entities and convey meaningful and actionable information to all relevant parties.

There are two capability statements in the communications domain:

The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)

The ability to communicate with responders in any environmental condition is crucial because communications enable safe and effective catastrophic incident response. Coordinating the efforts of emergency managers, civic leaders, responders and the public depends on timely, reliable and effective modes of communication. During a catastrophic incident, communications will involve an increased number of responders, jurisdictions and systems across a vast geographic area. Deficiencies in communications capacity, interoperability or infrastructure can strain or overwhelm steady-state capabilities; all of these deficiencies are exacerbated during large-scale incidents. Responders' ability to communicate with each other has a significant impact on operational efficiency and safety. Message transmission or clarity can be substantially reduced when operating in certain environments, particularly inside buildings, tunnels, underground spaces or over long distances. Significant research has been done to help improve communication systems that operate effectively in all environments; however, most response agencies still lack this capability.

Subject matter experts identified three RTOs that correspond with this capability:

- Voice and Data Communications Through All Physical and Electronic Environments
- Disaster Resistant Communications Systems
- Graceful Degradation of Communications Signals

Communications systems that are hands-free and ergonomically optimized and can be integrated into PPE

Most response agencies rely on land mobile radio systems that require a push button to transmit messages and use an attached speaker to broadcast received communications. While these systems may function effectively most of the time, it may be difficult to use them during tactical activities. Some radio systems offer a hands-free option, but responders continue to report that communications systems hinder their ability to perform tasks. In addition, radio systems add weight to the burden already carried by many responders. Integrating communications systems with PPE garments and equipment has the potential to improve the efficiency and effectiveness of response operations, improve communications clarity, and reduce the number of devices responders need to carry.

Subject matter experts identified one RTO that corresponds with this capability:

- Multi-sensory Communications Systems Integrated with PPE

Voice and Data Communications Through All Physical and Electronic Environments

Relevance: Some environments are conducive to sending and receiving communications, but others pose significant challenges. For example, communications can be difficult inside buildings, tunnels or underground spaces. Communications may also be degraded if equipment and infrastructure have been damaged by the incident. Regardless of the operating environment, emergency responders must be able to seamlessly send or receive orders and information, provide tactical updates, request help and receive warnings about hazardous or changing conditions. Therefore, the need to ensure verbal and digital communication through all physical and electronic environments is essential.

An additional component of this RTO is the transmission of sensor and other field-based data to incident command. An effective response requires the availability of pertinent information for decision-making. This information must be accurate, actionable and received as quickly as possible in an evolving response environment. Advances in technology will produce additional data streams, all containing information that may be necessary for incident command or on-scene responders.

Current Capability: The ability to transmit verbal and digital communications through all physical and electronic environments varies widely among response agencies and jurisdictions. Most jurisdictions own the hardware and equipment to communicate via push-to-talk radios and maintain limited network connectivity within their system. Agencies with larger budgets are able to deploy integrated repeater networks to transmit and amplify signals in areas where there otherwise would be a dead zone or degraded communications. These repeaters amplify signals so that it can be retransmitted over hills or past barriers. New York City has invested in a private long-term evolution (LTE) network to provide coverage for nearly the entire city. However, the ability to deploy a series of repeaters and utilize a private network is not the typical standard in all U.S. jurisdictions. In fact, most jurisdictions simply do not possess the capability to consistently communicate in all environmental conditions.

Despite advances in this field, new technologies are not often developed or tailored for the unique needs of the field of emergency response. Many state-of-the-art technologies are available to the general public (for example, smartphones that provide network connectivity and immediate access to data). However, these technologies were not developed to address the unique conditions of emergency response, so they cannot be effectively utilized in unpredictable and varying response conditions.

Responder Goals:

- Communicate through all environments, including inside buildings, underground and through physical barriers

- Rapidly-deployable (within 15 minutes)
- Portable components
- Powered using multiple sources including those on the incident scene
- Utilizes the existing infrastructure within buildings to enhance or amplify signals or clarity of communications
- Uses different bands across multiple systems without having several pieces of equipment
- Encrypted and secure
- Separate frequencies for emergencies and mayday-type alerts (for example, PASS)
- Effective communication in remote areas
- Provides enhanced quality and clarity of voice communication in all verbal transmissions

State of Technology: Many advances in the communications field have applicability to the operational needs of the response community. Technology is continuously being improved to include stronger signals capable of transmitting through challenging operational environments, such as through barriers and underground. The state of the art for verbal and digital communications includes various types of technology, including cellular and satellite communications, repeaters, mesh networks and cellular on wheels (COWs). All of these technologies have benefits and limitations with regard to responders being able to communicate in catastrophic conditions.

Radio frequencies (for example, cellular and satellite communications) – Communications devices such as a responder hand-held radio, walkie-talkie, cellphone, or satellite phone use RFs to connect with either terrestrial towers or a satellite in orbit to support voice, SMS and low-bandwidth Internet access. These devices operate using ultra-high-frequency (UHF) radio waves that propagate by line of sight. These radio waves can be easily degraded or blocked by hills, buildings, multipath radio wave interference or other barriers on an incident scene. Although satellite devices require line of sight, they are typically used in remote areas where cellular towers are not available, but there is access to open sky without obstruction. When barriers exist, a signal can be enhanced with the use of signal repeaters. However, there is a trade-off between transmission power and the available data rate. To maintain a given signal strength, power needs to be increased as distance between the device and the transmitter increases.

Mobile cell sites – Mobile cell sites such as COWs, cell on light trucks (COLTs) and cell in a box (CIAB) can be used in areas where cellular network coverage needs to be expanded or established. These technologies are similar to fixed cellular towers but are temporary installations. They are available in different sizes that can handle a range of signal loads and are deployable on varying platforms, such as a box or a truck. The range of a cell tower depends on a number of factors, including the height and direction of antennae, frequency of signal, power strength, ambient weather and absorption of environment (for example, building, vegetation).

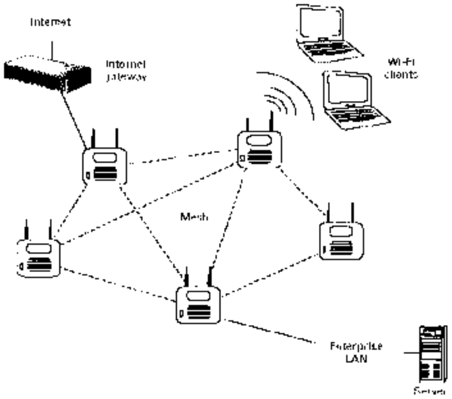


Figure 11. Mesh Network Diagram

Signal repeaters (also known as breadcrumbs) – Wireless communication devices that utilize radio waves can be boosted using signal amplifiers or perpetuated using various types of antennas. Repeaters are used to continue a signal in areas where it would otherwise be blocked or degraded (for example, inside a building or around a barrier). The repeaters work by collecting a signal and then retransmitting it in a much smaller scale to a cellular tower. Repeater use is increasing rapidly, and so are advances in the technology of size, weight and signal strength. For example, DHS is investing in a project to develop a very small (one-inch square, half-inch thick) repeater that is both waterproof and heat-resistant up to 500 degrees. This type of signal repeater was designed specifically to develop a network in signal-denied environments for the emergency response community.

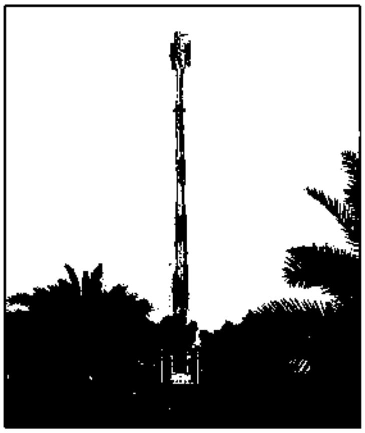


Figure 12. Cell on Wheels

Mesh networks – Similar to repeaters that propagate signal, devices such as laptops, cellphones and other wireless devices can link as radio nodes. This is called a mesh network. This means that only one node needs to be wired or connected to a network connection and other wireless devices can link to it (instead of a cellular tower) and act as routers to send data using the built-in Wi-Fi transmitters. Each device, or "mesh node," uses routing protocols to determine whether to keep the data it receives or pass it along to the next device until a destination is reached. Therefore, each device only needs to transmit the data as far as the next node in the network instead of to a cell tower or satellite. If one node drops out of the network, the data can quickly find another. There are two main advantages for responders to use mesh networks. First, they can leverage radio physics to pass information through signal-denied environments and across long distances. Second, they can use sophisticated triangulation and time-of-flight algorithms to determine the location of nodes and users in the network, such as responders on an incident scene. The limitations of mesh networks include the sophistication of the network setup, maintenance and the availability of nodes in a given area.

FirstNet

In addition to these technologies, an effort is underway to revolutionize multiple aspects of emergency responder communications. The First Responder Authority Network (FirstNet) is an independent authority within the National Telecommunications and Information Administration that is tasked to "provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety."[51]

FirstNet is focused on enhancing and optimizing operational capability through the development of a new Band Class 14 network. To develop this network, Congress allocated 20 MHz of radio spectrum to FirstNet, and responders will have priority or preemptive access to the system during response operations. Each state will develop an individual radio access network that connects to the FirstNet core network.

FirstNet will employ LTE technology that incorporates a radio access network (RAN). RAN is the component of LTE that includes cell towers as well as mobile hotspots in vehicles that can connect to the core network over satellite or other types of wireless infrastructure.[52] This technology should improve communication coverage for emergency responders, including coverage in challenging operating environments.

Improving the ability to transmit information in challenging environmental conditions is a shared goal among many disciplines. The U.S. military is funding multiple efforts that may benefit the response community. A small number of the most pertinent efforts are described here. DARPA currently has a funded program called the A-to-I Look-Through program to help advance this complex issue.[53] The goal of this program is to improve the operational bandwidth, linearity, and efficiency of electronic systems when the desired outcome is to receive and transmit information using electromagnetic (radio) waves, especially under extreme size, weight, power and environmental conditions. This program will rely upon developing new electronic processing subsystems methods and architectures based on new understandings of mathematical principles and embedded signal processing.

DARPA often initiates challenges to motivate teams of researchers to make progress in certain areas. It has initiated the Spectrum Challenge to help develop innovative approaches to adaptive, software-based radio communications in multi-user environments. The Spectrum Challenge was issued to address the fact that "first responder radios need to be able to communicate reliably in such congested and contested environments and to share radio spectrum without direct coordination or spectrum preplanning."[54] The ultimate goal is to develop protocols for radio software that will indicate the best communication channels when there are multiple interfering signals.

[51] "About FirstNet," First Responder Network Authority, last updated: n.d., http://www.firstnet.gov.

[52] Ibid.

[53] "Analog to Information Look Through," DARPA: Microsystems Technology Office, last updated: n.d, http://www.darpa.mil/Our_Work/MTO/Programs/Analog-to-Information_(A-TO-I)_Look_Through.aspx.

[54] "Spectrum Challenge," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/Spectrum_Challenge.aspx.

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

- FirstNet is still in the early development stage, and the time frame until implementation has not been determined. Different states are exploring different approaches to create the required radio access networks.
- Each state faces political, governance and local control issues for management of their radio access network.
- Manufacturers will have to develop devices that have access to the new frequency band.
- FirstNet will initially focus on data transmission and interoperability. Response agencies will continue to use land mobile radio systems for voice communications. Voice over LTE (VoLTE) will likely replace land mobile radio systems at some point, but this capability will require longer-term development.
- Responders anticipate significant challenges with building the backhaul infrastructure large enough to support public safety requirements an efficient allocation of the spectrum.

Disaster Resistant Communications Systems

Relevance: Effective response requires the capability to provide reliable, coordinated communications—including secure and nonsecure data, video and voice—among and across levels of the government and response community. However, catastrophic incidents have the ability to significantly damage or completely destroy the communications infrastructure and systems used by emergency responders. For example, incidents such as a nuclear detonation produce an electromagnetic pulse (EMP). An EMP can cause serious disruption and widespread damage to electronic devices and networks, including communications systems and technology equipment.

A nuclear detonation or use of an EMP device is a low-likelihood incident, but even incidents that involve more routine threats or common operating environments can have devastating effects on communications systems. Extreme heat or cold, high winds or water can also critically damage equipment and networks.

Current Capability: Public safety radio systems are ruggedized to provide protection against commonly encountered hazards. Radios used by the fire service generally have a higher degree of thermal protection, while radios used in marine environments are waterproof or water resistant. However, standard radio systems used regularly by emergency responders do not protect against EMP or extreme conditions. Further, communications systems include more than just the radios. The towers, repeaters and other equipment must also be disaster resistant. In many cases, this part of the communications infrastructure is most vulnerable. Following Hurricane Sandy, for example, 25 percent of cell towers were inoperable within 12 hours of the event. One solution is for radios to be stored in boxes hardened to shield the effects of an EMP. However, it is not operationally feasible to place all daily-use radios in boxes when not being actively used. Purchasing a separate set of radios that can be stored in preparation for an event is not financially possible for most jurisdictions. Many jurisdictions maintain a cadre of amateur radio (also called ham radio) operators. Amateur radio has dedicated bands, reserved by the Federal Communications Commission (FCC), that have frequently been used to support response operations.

Technologies including communication facilities, towers, radios, repeaters and other equipment are hardened against adverse effects from catastrophic incidents at varying levels. For example, some facilities have taken measures to include using flame-resistant materials, carefully selected locations that are elevated yet stable and resistance to high-powered winds. Other disaster resistant technologies include repeaters that are built with heat resistance for use in firefighting scenarios. Most cell towers also include backup batteries and sometimes generators to withstand power outages.

Responder Goals:

- Public safety grade communications infrastructure (including radios, towers, repeaters and other necessary equipment) against conditions such as electromagnetic pulse, heat, blast, water and extreme temperatures[55]
- Rapidly deployable (within 15 minutes)
- Intrinsically safe and ruggedized components
- Easily portable components

State of technology: DOD maintains a number of military standards regarding EMP preparedness. Many critical defense systems comply with nuclear survivability and hardening requirements, which protect against EMP threats. DTRA continues to conduct EMP assessments on the critical power infrastructure, specifically the power grid and telecommunications networks. However, there has been limited transition of military capability in this area to emergency response applications. Research has also been done to develop electrical cables that are insulated and shielded from electromagnetic interference to protect electronic devices. For devices that are not hardened, storage options offer protection to critical items. However, because it is not possible to predict the size, strength and proximity of an EMP, it is unclear what level of protection exists.

DARPA has programs dedicated to enhancing reliable, secure and resilient communications. One such program is the Safer Warfighter Communications (SAFER)

[55] "Public safety grade" refers to the hardening of network components to ensure that the communications systems of emergency response agencies will remain operational during and immediately following a major natural or manmade disaster on a local, regional, and nationwide basis. "Defining Public Safety Grade Systems and Facilities", National Public Safety Telecommunications Council. May, 2014.

program.[56] The goal of this program is to develop technology that enables safe and resilient communication over the Internet. The technology will also enhance applications such as instant messaging, email, social networking, streaming video, voice over Internet protocol (VoIP), video conferencing and other media that promote effective communication.

Additional research is ongoing to develop survivable communications networks that can provide connectivity in the absence of power and network connectivity. One system relies on creating open-source tools that will allow citizens to use their existing infrastructure as part of a rapidly deployed network to meet basic communications needs. The system includes small modules powered by small solar panels or previously powered large electronic devices (such as a hybrid motor vehicle) that can be acquired by citizens or civic groups to provide ad hoc communications capability when needed.

Potential Challenges:

- Responders are concerned about the costs of an EMP-hardened radio system, anticipating high costs for a low-probability event. Purchasing these radios may not be feasible in the financially constrained environment that currently exists for many jurisdictions.
- Public safety communications may rely on commercial cellular or wireless networks and equipment, which are also not hardened against EMP effects. Development of a civilian standard will be sufficient only if commercial carriers also harden their systems.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Graceful Degradation of Communications Signals

Relevance: While responders rely on communications for incident response, they are aware that there are times when the communication signal will become so weak, or completely lost, that transmission is no longer possible. However, it is not possible to predict when the communication signal will be lost, and responders are often in the position of not realizing they are no longer transmitting until they do not receive a response. This "no-notice" loss of signal can cause a lack of transmission in critical incident information and can place the responder's life in danger.

There is a need for responders to have more notice on the status and degradation speed of their communication signal and a more graceful degradation of the signals. This would allow responders to adapt quickly to the pending lack of communications and transmit critical pieces of information before losing connectivity.

[56] "Safer Warfighter Communications," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/SAFER_Warfighter_Communications_(SAFER).aspx.

Current Capability: Responders described the current degradation as "a point where communication just falls off," meaning that there is currently no capability, with limited exception of a screen display similar to the reception bars on a typical cellphone, to alert the responder to a diminishing signal. A screen display is not ideal, as emergency responders cannot constantly look at a visual indicator while simultaneously transmitting information.

The strength signal itself does not allow for reduced communications, it simply goes from fully functioning to not transmitting anything. Responders are not afforded an opportunity to transmit shorter or more concise verbal message as the signal degrades. There is no gradient or step-wise loss of functionality.

Responder Goals:

- Alerts for the degradation level with corresponding effectiveness level (an indication of how well messages are being transmitted)
- Audio indicator when the signal is lost completely
- Directional interface that guides responders toward stronger signal strength
- Ability to poll on-scene radios for signal status to determine if the user is losing reception
- Enhanced capability that functions with current technologies

State of Technology: Some radios and cellphones have preset text messages that can be used in lieu of voice transmission when signals become very weak. These devices typically switch to a text system and can send out a small amount of texts that are preprogrammed with short commands, alerts or maydays. In addition, some radios can automatically switch bands and search for the strongest repeater or tower every 15 seconds, depending on the strength of the signal, helping to maintain signal strength.

DARPA established the Adaptive RF Technology (ART) program to advance the hardware used in hand-held communication radios.[57] DARPA is developing a fully adaptive and reconfigurable framework that is agnostic to specified waveforms and standards. DARPA believes that this will enable the individual warfighter, using a small-scale unmanned platform to analyze and characterize the signal environments. This will allow the warfighter to determine the signal strength and changing conditions.

[57] "Adaptive RF Technologies," DARPA: Microsystems Technology Office, last updated: n.d., http://www.darpa.mil/Our_Work/MTO/Programs/Adaptive_RF_Technologies_(ART).aspx.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Potential Challenges:

- Responders are concerned that adding features or improvements may increase the size and weight of existing systems. The goal is to increase the performance of PPE, including communication devices, without adding size or weight.

Multi-sensory Communications Systems Integrated with PPE

Relevance: The standard communications platform employed by the vast majority of response agencies is a hand-held push-to-talk radio used for verbal communications. These types of radios clip onto the exterior uniform or protective garments of responders. Recent developments in multimodal interfaces and displays are expanding the possibility of more sophisticated communications mechanisms that rely on multiple senses, such as sight, hearing and touch. As part of this RTO, responders would like to receive and access information visually. They would like to see a display of key operational and physiological data and information. This could include life-safety data, such as the amount of oxygen remaining in a self-contained breathing apparatus (SCBA) tank or blueprints or schematics for the building in which they are working. They would also like to be able to identify the location of other responders, resources and hazards/threats, both within and beyond their field of view. Responders could also receive just-in-time training or instruction via visual display.

Current Capability: As mentioned, most response agencies rely on land mobile radio systems that require a push button to transmit messages and use an attached speaker to broadcast received communications. Responders reported that it is often difficult to use these radios during tactical activities. For example, a firefighter operating in full protective gear, including breathing apparatus and heavy gloves, may find it difficult to transmit a message while dragging a hose line or carrying tools or to receive a communication due to sound dampening from the SCBA mask and loud ambient noise. Radio devices currently exist that can be operated using hands-free features, often through the use of bone-conduction microphones that transmit sound through the bones of the skull into the inner ear. However, performance is often still degraded by the noise of the incident scene. Some headgear worn by firefighters or SWAT teams integrates communications equipment, but other factors degrade the clarity of these communications.

Responder Goals:

- Equipment integrates into PPE or other existing equipment with minimal or no net weight gain for the responder

- Hands-free activation
- Multiple configurations based on the needs of each discipline
- Minimal SWP
- Noise-filtering mechanism that accounts for significant ambient noise
- Multi-sensory display of information, including key operational and physiological data and information
- Ruggedized, waterproof, thermal resistant, intrinsically safe, simple, and not able to be turned off by the user
- Integrates into PPE for all disciplines

State of Technology: The technology to support a heads-up display (HUD) for responders to send and receive information is widely available. HUDs are also used by the general public for a variety of purposes, such as displaying speed and distance on a car on the windshield while the car is in motion. They are also used extensively in aircraft to display needed pieces of information.

While HUDs are not routinely used in emergency response, the technology could be tailored to the unique needs of each response discipline. DHS S&T, for example, has funded the development of a thermal HUD for use by firefighters. This HUD helps to address the need for firefighters to be able to monitor their internal and external temperatures, which is difficult when they don level-A hazmat suits. When dangerous thermal levels are reached, this particular HUD provides the firefighter with an alert. [58]

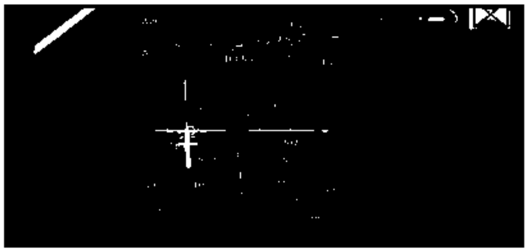


Figure 13. Information Available in HUD

There are several other opportunities for advancement in this area, including the transition of HUD systems developed by DOD for the warfighter, as well as commercial development of products such as Google Glass. Users can see information such as maps, temperature and logistical information in their line of sight while wearing the glasses. Applications have already been developed specifically for the fire and law enforcement disciplines using the Google Glass platform. Researchers are exploring the integration of this technology into the face shield of responders' helmets and headgear.

The U.S. military continually invests in programs that help to advance the way in which warfighters are able to visualize their operating environments. As part of this effort, DARPA established the Urban Leader Tactical Response, Awareness and Visualization

[58] "S&T Project Roundup What We Worked on in September 2013," FirstResponder.gov, last updated: n.d., http://www.firstresponder.gov/SitePages/ResponderNews/Article.aspx?s=Articles&itemID=192.

(ULTRA-Vis) program.[59] Under this program, a prototype for an augmented reality system was developed. Essentially, soldiers are able to use this prototype to overlay full-color graphical iconography onto the local scene observed by the soldier. This is accomplished by integrating a lightweight, low-power holographic see-through display with a vision-enabled position and orientation tracking system on the solider. In doing so, warfighters are able to increase their understanding of the areas and visualization of threats.

Advances are also expected in the use of bone-conduction technology. Commercial providers expect to release headsets that incorporate a bone-conduction microphone, allowing two-way communication. This would allow responders to send and receive communications without a device blocking the ear and preventing the reception of other ambient sounds.

Potential Challenges:

- Responders are concerned about the vulnerability and security of communications when using wireless connectivity.
- Google Glass is not ruggedized for the requirements of the incident scene.

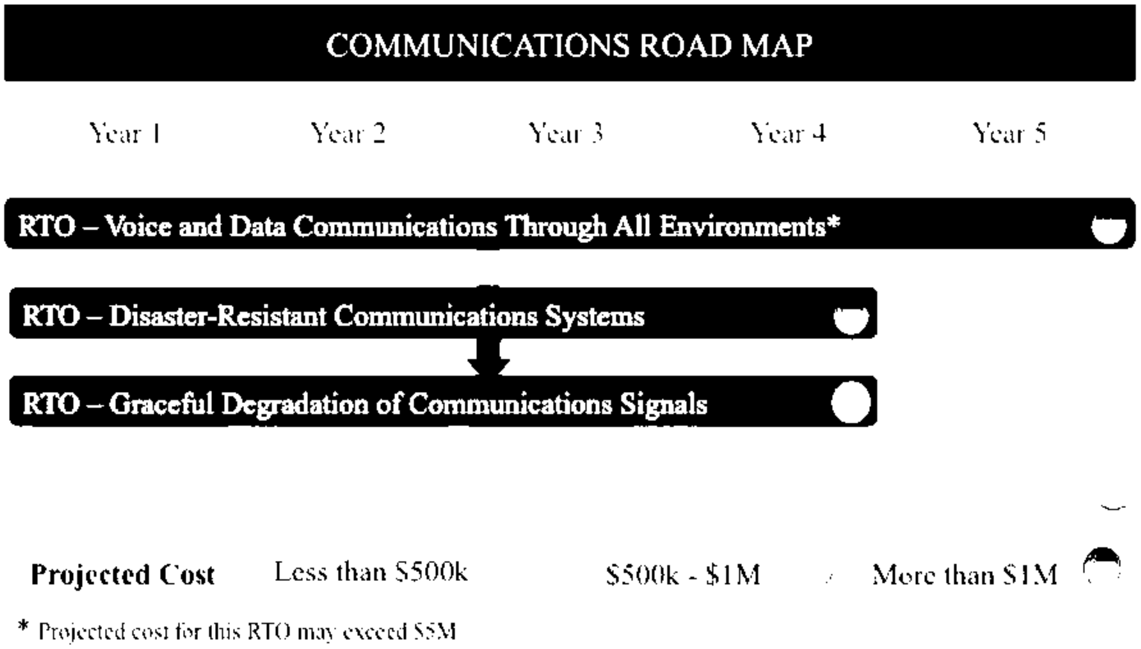
Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Communications Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the communications RTOs above.

- Develop public safety grade VoLTE systems for public safety use
- Develop a civilian EMP survivability standard to which public safety communications systems can be built
- Collect requirements for and integrate a signal indicator into existing radio equipment
- Transition adaptive RF technology being developed for military applications to emergency response applications

[59] "Urban Leader Tactical Response, Awareness and Visualization," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/Urban_Leader_Tactical_Response,_Awareness,__Visualization_(ULTRA-VIS).aspx.



COMMUNICATIONS ROAD MAP

Year 1 Year 2 Year 3 Year 4 Year 5

RTO – Voice and Data Communications Through All Environments*

RTO – Disaster-Resistant Communications Systems

RTO – Graceful Degradation of Communications Signals

Projected Cost Less than $500k $500k - $1M More than $1M

* Projected cost for this RTO may exceed $5M

Figure 14. Communications Technology Road Map

Command, control and coordination is defined as the ability to identify incident priorities, allocate scarce resources and exchange relevant information to make effective decisions in a stressful environment.

There are three capability statements in this domain:

The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time

Incident commanders are responsible for setting objectives and assigning tasks to efficiently respond to emergencies. The number of tasks and personnel scale with the size of an incident; therefore, catastrophic events may be difficult to manage without the aid of technology. Incident commanders need the ability to know the progress of tasks and to have up-to-date situational awareness to manage within a complex workflow environment. Incident commanders can effectively re-task personnel or allocate additional resources if they can monitor responder actions and tasks. Ideally, incident commanders would be able to achieve this level of command and control with little burden on the responders in the field. Therefore, tactical actions of responders and other information should be remotely collected without impeding or degrading the performance of existing communications. Responder actions also need to be monitored in real time and integrated into a holistic workflow management system that tracks the level of completeness for each assigned task.

Subject matter experts identified two RTOs that correspond with this capability:

- Real-time Monitoring of Responder Actions
- Intelligent Integrated Workflow System

The ability to identify trends, patterns and important content from large volumes of information from multiple sources (including nontraditional sources) to support incident decision-making

The digital age has increased the availability of and access to data that could help inform emergency response operations. During catastrophic incidents, responders can be overwhelmed by the amount of incoming data from both traditional and nontraditional sources. Successful utilization of this data depends on the ability to collect, aggregate, validate, analyze and disseminate incident-specific data and information. Responders require a system capable of ingesting large amounts of data, identifying emerging trends and patterns and filtering for key information. Such a system would not replace human analysis, but would act as a decision support tool to assist both analysts and decision-makers.

Subject matter experts identified three RTOs that correspond with this capability:

- All-source Information Analysis System
- Real-time Predictive Analysis and Modeling
- Incident-scene Information Recognition and Pattern Analysis

The ability to identify, assess and validate emergency-response-related software applications

As technology advances, so do the support tools available to emergency responders. Although some of these support tools are hardware, many are in the form of computer software, including applications that help the responder prepare for, respond to and recover from catastrophic incidents. Software designed to support emergency responders provides timely, critical and accurate information regarding a range of threats and response actions. Responders need to be able to trust that these applications provide valid information, function when necessary, operate on all relevant platforms and protect sensitive information.

Subject matter experts identified three RTOs that correspond with this capability:

- Core Requirements Standard for Response-related Software Applications
- Software Development Kit for Integration of Response-related Software Applications
- Platform for User Evaluation of Response-related Applications

Real-time Monitoring of Responder Actions

Relevance: Incident command is responsible not only for developing strategic and tactical plans, but also for ensuring that those plans are implemented and the associated tasks are carried out. Incident commanders may be overwhelmed by the complexity of catastrophic incidents and may not be able to effectively monitor the actions and progress of the response. Incident command would like to be able to track the progress of teams and individual responders in completing the missions to which they have been assigned. This would allow decision-makers to identify when a mission needs more resources and when responders can be directed to other tasks.

Current Capability: At this time, there is no commonly used tool for monitoring responder actions on scene. Existing capabilities rely largely on voice communication between responders and the incident commander, particularly through the transmission of information requests and progress reports. While this practice allows the incident commander to receive on-demand updates, the reliance on voice communication can detract from overall mission success and responder safety.

This is due to two main factors:

- Potential unreliability of communications systems in certain situations (such as when operating in wide geographic areas or inside buildings)
- Continuous changes in the incident scene (potentially limiting the accuracy of transmitted messages)

The capability to remotely monitor actions and progress could resolve these concerns by providing real-time information and increased reliability that improve decision-making.

Commonly used computer-aided dispatch (CAD) systems are able to visually monitor the progress and location of emergency response vehicles. These systems use a transponder affixed to the apparatus to provide real-time updates of the location of vehicles. CAD systems also work with mobile data computers (MDCs) that are installed in many response vehicles. Responders are able to update their status via the MDC, which provides updates in the CAD system.

Responder Goals:

- Automated system to collect tactical inputs from individual responders in real time
- Includes preset command features to translate verbalized tactical actions into status updates (for example, need more resources, task complete) to limit the burden of effort on the responder to use push-to-talk radios during an incident
- Integrates the status of all responders into a common operating picture on a dashboard for command visibility
- Displays tasks in an automated sliding scale that adjusts based on task completion
- Includes customizable settings, including task lists and timers for each task
- Includes an override feature for an administrative user to update the status when a responder cannot make updates
- Relays information in real time to incident command, caches data when connectivity is offline and automatically forwards data when the connection is restored
- Does not interfere with other radio communications
- Provides appropriate SWP to provide functionality but does not place an extra burden on the responder
- Interoperable and easily integrated with other monitoring or communications equipment
- Scalable to quickly add responders during an incident

State of Technology: Development efforts are underway to extend the visual display of vehicles that exists with modern CAD systems to personnel. Existing systems are able to notify personnel that they have been called into service via an application on their mobile device. Responders confirm receipt, and the system tracks their progress toward the incident scene via cellular and wireless networks. Responders are able to send and receive communications, which can be used to relay and update tasking orders. Current products are unable to track the completion or activities at the task level. However, development efforts underway include products that can incorporate pre-plan information, which could potentially be used to track tactical progress, and can be integrated with other electronic situational awareness systems.

Other commercially available software systems help manage and track resources, including personnel, throughout incident response. As described above, tracking the progress of personnel working on assigned tasks requires check-ins from the field. These check-ins can be automatically categorized and updated on an incident manager's status boards, which include event logs, unit logs, operating procedure status tables and situation reports. These systems allow commanders to establish incident objectives (for example, organizational or division assignments, medical plans, communications strategies, safety messages).

Note: The state of technology for real-time tracking of responder location and display on a common operating platform can be found in the "Indoor Responder Geolocation" and "Outdoor Responder Geolocation" RTO discussions.

Potential Challenges:

- Current systems rely on connectivity at the incident scene, but this is far from guaranteed. Developers are currently working on offline options that will allow information to be cached and then forwarded when connectivity is restored, but that functionality is not yet available.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Intelligent Integrated Workflow System

Relevance: When on scene, responders are focused on tasks related to saving lives and mitigating threats. The role of an incident commander is, in part, to monitor task progress and the workflow until the objectives are met. The term *intelligent integrated workflow* refers to a system that automates portions of the monitoring and management to expedite the process. With insight into the workflow, incident commanders can anticipate resource demands or reassign assets to other tasks. Incident commanders must be able to visualize this information in real time on a common operating platform. This capability could reduce the amount of time an incident commander spends analyzing vast amounts of incident data and situational awareness reports to focus on managing the response.

Current Capability: Research and responder input uncovered no known intelligent workflow systems focused on the emergency response mission. Task progress is typically communicated using hand-held radios or MDCs from responders in the field to incident commanders and dispatch operators. Some CAD systems are able to analyze response data to produce helpful information and statistics, such as average response time until units are on scene, but responders currently have no capability to automate or provide decision support to workflows.

Responder Goals:

- Identifies and collects key tasks associated with incident response for integration into an electronic workflow system
- Incorporates data from previous incidents for machine learning and prediction
- Integrates with logistics situational awareness systems
- Automates task management where possible to reduce responder interaction where applicable
- Tracks responders' previous system inputs
- Automates user choices or proposed next steps based on task progress
- Generates alerts to inform or predict the next actions that should be taken
- Includes customizable graphic displays
- Customizable to allow administrator to input jurisdiction-specific standard operating procedures
- Includes a confidence or quality control feature to assist decision-makers

State of Technology: Intelligent workflow systems are used extensively in other fields, for both automated and manual processes to capture and digitize processes and standard operating procedures and provide an audit trail of activities. Many of these systems are able to monitor the submission, processing and real-time tracking of requests. They can designate and prioritize the status of tasks (for example, assigned, past due, completed), provide alerts when processes are delayed or interrupted and provide graphic displays of workflows with real-time visualization.

Some of the commercially available incident management systems can provide commanders with support for workflow management and automate parts of the process, but these tools need to be customized for use at the jurisdictional level. For example, technologies are being developed that can help automate workflows based on the progress of tasks in the field and a specific jurisdiction's pre-planned standard operating procedures. The systems suggest courses of action that are aligned with local operating procedures, National Incident Management System (NIMS) and Incident Command System (ICS) processes and that incorporate FEMA's resource management life-cycle information. The workflow automation converts incoming messages from the field into action-based message types such as status update, request for action and resource request. These messages can then be tracked and managed within the system. Incident command can then make official requests and follow up to ensure tasks are being completed.

Potential Challenges:

- The ability to automate the content of notifications beyond binning into message categories is limited.
- Verifying that tasks are complete is still reliant on responder reporting. Some systems include the ability to upload images, but this functionality is not yet automated for responder applications.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

All-source Information Analysis System

Relevance: A catastrophic incident generates a lot of information that needs to be collected, analyzed and stored for decision support. This information is necessary for critical lifesaving and operational decisions, but it is transmitted in a multitude of different formats. Some require advanced knowledge or training to interpret. Response agencies will be held accountable for using this information, and it must be available in a comprehensible and concise format. Responders would like a common platform that can filter, aggregate and correlate data into an output that is relevant and usable for the decision-maker. Outputs and visualizations should be in a format that can translate the analysis of the data into actionable information.

Current Capability: Many response agencies use electronic incident management systems to support decision-making during response operations. The most commonly used systems utilize a dashboard system, which allows incident command to view different functions in a series of layers or tabs on the display. When this information is aggregated, incident commanders have a better common operating picture. However, they still lack the analytical and decision support modeling function requested by responders.

State and major urban area fusion centers provide additional capability for information integration and analysis. Fusion centers are collaborative efforts between multiple agencies to share information among federal, state, local and tribal organizations. The fusion centers are primarily focused on the analysis of threat-related information to prevent incidents but can be used to improve situational awareness and decision-making during response operations.

Responder Goals:

- Integrates a baseline set of business rules for every emergency management agency with the ability to customize for specific events or types of incidents
- Automatically filters, aggregates and correlates data
- Ability to graphically display and visualize data
- Includes predictive analysis to optimize courses of action (for example, rerouting assets, choosing to shelter versus evacuate)

- Aggregates data at a speed to inform real-time decision-making
- Integrates natural language processing to aggregate large amounts of text data to ease decision-making
- Customizable business rules for discipline-specific needs
- Filters information to ensure relevant, actionable information
- Includes a customizable graphical user interface (GUI)
- Includes next-step suggestions or considerations based on analytic outputs

State of Technology: Integrated tools that provide all-source information management, analysis and decision support either are in development or require customization, testing and evaluation before being used by emergency responders. Existing COTS systems do not meet the responder requirements, which include real-time aggregation, analysis and optimization of decision-making with predictive analyses. Most existing systems can automate functions for ingesting and mashing data but are very limited with regard to analysis and decision support. In addition, many of these functions are not rapid and require special programming support from developers.

The volume of incoming data increases during times of crisis, and systems need to be designed to rapidly detect changes in the data patterns and trending topics as events unfold. These technologies should provide meaningful analysis of streaming social media and other data to the end user in real time. To this end, DARPA has been developing a tool called Insight to consume and process information and provide mission-relevant, timely insights to incident commanders.[60] The goal of this program is to use technology and automation to enhance an individual's ability to support real-time operations with actionable data. Insight is designed to receive, index and store incoming data from multiple sources and analyze and correlate that information. Furthermore, DARPA is working to incorporate behavioral learning and prediction algorithms to help analysts discover and identify potential threats and corresponding activities.

Natural language processing (NLP) can assist analysts in understanding the content of social media data for the purposes of sentiment analysis, topic modeling, trend analysis and social network analysis. NLP uses machine learning algorithms to enable software to derive meaning from a user's input. The ability to use NLP lends itself to many different system features such as custom alerts, changes

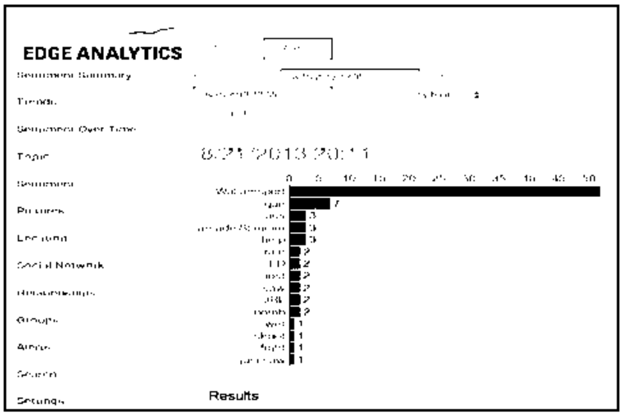


Figure 15. Edge Analytics Interface

[60] "INSIGHT," DARPA: Information Innovation Office, last updated: n.d., http://www.darpa.mil/Our_Work/I2O/Programs/Insight.aspx.

in data patterns, understanding local context, sentiment analysis and topic modeling.

Although real-time analytics technologies are still maturing, many of the features that emergency responders desire (such as sentiment analysis, filtering based on geolocation, social network representations, identifying influencers, custom alerting, trend and pattern analysis and topic modeling) already exist. An example of this is shown in figure 15 using a tool called Edge Analytics (EA). EA was initially developed by a DOD Federally Funded Research and Development Center (FFRDC) and has been piloted in various environments to conduct social media analytics. Figure 15 displays EA's real-time filtering and topic modeling capabilities. Advancements are still necessary in the areas of data fusion, natural language processing and real-time analysis to create a robust all-source analysis tool. These research areas are currently in development.

Potential Challenges:

- The appropriate entity to provide governance and maintenance support for an all-source information analysis system is undetermined.
- The accuracy of machine learning and NLP needs improvement.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Real-time Predictive Analysis and Modeling

Relevance: Response agencies conduct pre-planning efforts and exercises to improve their ability to respond to an incident before it happens. From these activities and past operations, they are able to predict certain factors in how an incident might unfold. However, there are many incident-specific variables that significantly impact incident action planning, including the population of the affected area, the existing and evolving hazards posed by the type of incident and the presence of other effects or hazards. There are ongoing and well-established efforts by the federal government to conduct predictive analysis for various types of threats including hurricane, flood and earthquake modeling. However, the emergency response community is lacking a baseline, customizable, all-hazards predictive analytic approach and integration strategy. Responders would like the ability to easily integrate incident-specific information with available models into decision-making processes in near real time.

Current Capability: There are many sophisticated models that can estimate effects related to natural and man-made incidents, including hurricanes, wildland fires, earthquakes, disease outbreaks, evacuations and population behaviors. Generally, each of these models is developed by different organizations or agencies working from disparate information sources. One example of modeling software used to estimate natural events is from the National Hurricane Center (NHC). This software creates hurricane track and intensity models and is used to inform emergency response efforts. NHC is an example of a modeling source that incorporates historical data and real-time information to develop alerts, warnings, forecasts and predictive analyses that help inform decision-making related to potential weather threats.

Some of these models can be accessed through an integrated suite called Standard Unified Modeling, Mapping, and Integration Toolkit (SUMMIT). The goal of SUMMIT is to create a collaborative environment that links the leading modeling and simulation tools and data to help emergency responders train for and respond to incidents.[61] SUMMIT has been used to support federal, state, regional and local exercises and operational planning efforts.

Another modeling resource for emergency responders is the DHS-led Interagency Modeling and Atmospheric Assessment Center (IMAAC). The IMAAC coordinates and disseminates federal atmospheric dispersion modeling and other hazard-prediction products.[62] These products provide information during actual or potential incidents involving hazmat releases.[63] The IMAAC provides emergency responders with predictions of hazards associated with atmospheric releases to aid in the decision-making process to protect the public and the environment.[64]

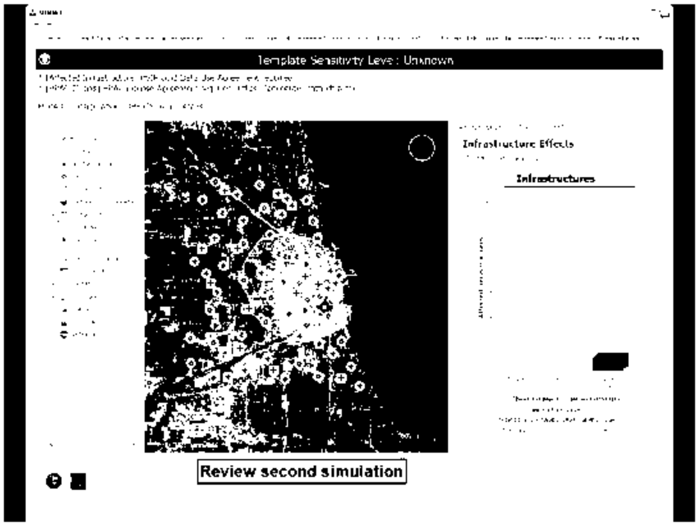


Figure 16. Standard Unified Modeling, Mapping, and Integration Toolkit

Responder Goals:

- Enhances model fidelity for threats such as chemical, biological, epidemiological, radiological, EMP, nuclear, explosives, fire and population dispersion.
- Incorporates high-performance analytics modeling of multiple data streams
- Conducts predictive analysis for specific incidents in near real time (for example, within one hour)

[61] "SUMMIT," DHS, last updated: n.d., https://dhs-summit.us.

[62] "Interagency Modeling and Atmospheric Assessment Center," DHS, last updated: October 25, 2013, http://www.dhs.gov/imaac.

[63] Ibid.

[64] Ibid.

- Integrates outputs into decision support tools and existing electronic situational awareness tools
- Enhances social network analysis
- Improves the fidelity and validity of data
- Generates and runs customized stochastic models[65]

State of Technology: Operations research and the science of simulating scenarios to inform decisions have been around for decades. Modeling has been used for predictive analysis for large and small events and continues to evolve in many different industries, including the military, space exploration, weather forecasting, and homeland security. The Department of Energy national laboratories have done extensive modeling in various areas that have application to catastrophic disaster response including fallout, blast effects in an urban environment, mass sheltering and evacuation and EMP effects from a nuclear event. These models are not operational at the local responder level to help inform immediate response actions.

To this end, S&T, in conjunction with FEMA and in collaboration with Sandia National Laboratories, is developing a geo-agile platform called SUMMIT that enables responders to use and integrate models to improve response planning, training, and exercises.[66] The tool has already been used in various international, national and regional exercise scenarios. Eventually, the goal is to utilize this suite of models to inform decision-making during response operations for catastrophic incidents. The SUMMIT framework is described as platform-neutral, which allows users to access the models from a Web browser and mobile applications.

SUMMIT is deployed through FEMA's National Exercise and Simulation Center (NESC) to provide state-of-the-art modeling and simulation capabilities to support national, federal, state, local and tribal exercises. Once SUMMIT has undergone the Software Engineering Life Cycle (SELC), Security and Compliance transition process through DHS S&T, the emergency management community will be able to utilize the tool. During this transition period, research and development efforts will continue to advance SUMMIT capabilities in preparation for future deployments to the FEMA NESC.[67]

[65] Stochastic models include at least one random variable. Stochastic models are used to estimate the probability of different outcomes.

[66] "SUMMIT," DHS, last updated: n.d., https://dhs-summit.us.

[67] Jalal Mapar, Keith Holtermann, et al., "The Role of Integrated Modeling and Simulation in Disaster Preparedness and Emergency Preparedness and Response: The SUMMIT Platform", Department of Homeland Security, 2012.

Potential Challenges:

Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

- Responders would like model projections and updates in real time. Delays from real time can be caused by interruptions in the currency and quality of sensor data and other pertinent information, some of which comes from third parties.

- Enhancements of model projections require continuous and real-time updates of sensor data from the incident scene. Communication system failures following a catastrophic event may constrain the transmission of sensor data.

Incident-scene Information Recognition and Pattern Analysis

Relevance: Responders must quickly make informed decisions based on credible incident-scene information, reports from the field, and historical data. The sheer volume of information that needs to be considered and analyzed can present challenges, especially during a catastrophic event. This RTO is related to a response organization's ability to identify specific information being developed on the incident scene and conduct pattern analysis to validate and inform tactical decision-making. This type of analysis can improve situational awareness and help forecast an incident's evolution. The evolution of an incident dictates what, where, and when additional resources should be deployed.

Current Capability: Human initiative and analysis are the principal tools utilized for this capability. This type of information recognition and pattern analysis is done in some law enforcement agencies with the integration of sensor technologies, such as light detection and ranging (LIDAR), geotagging or ground sensors, to monitor specific locations. However, it is not widely used by the responder community. Joint fusion centers act as one resource to encourage data aggregation and information sharing among agencies. Responders in the field employ methods such as predictive policing and social network monitoring depending on the initiative of the agency.[68] Data synthesis and analysis systems currently exist, but they have not been specifically customized for and used by the response community.

Responder Goals:

- Collects incident-specific information to provide enhanced situational awareness
- Analyzes information to provide predictive clues as to what cascading effects of the incident may occur
- Rapidly analyzes aggregated incident-related data

[68] Predictive policing is a forecasting technique to identify likely targets for police intervention. These analytic techniques are typically statistical predictions and quantitative in nature.

- Fuses data streams across various information sources (including soft and hard sensors)[69]
- Collects and analyzes metadata of streaming information
- Integrates information protocols and agreements
- Calculates a level of confidence in data
- Includes multiple sources of validated information
- Displays trend data statistically and across the incident timeline

State of Technology: The development of a disaster management system that can detect trends and patterns has been a topic of interest in the technology community over the last decade. Technologies exist that can identify trends over space and time, monitor resources and displays results for a specific geographic area. However, none fully address responder requirements for an all-inclusive incident scene trend and pattern analysis tool.

DHS has invested in several infrastructure protection and disaster management projects that relate to this RTO with regard to collection, analysis and visualization.[70] Specifically, advancements are being made to develop tools that rapidly collect, process, present and understand massive amounts of data from multiple sources, including database information, message traffic, text documents, imagery, video, sensor, and instrumentation data from an incident scene. These analytical tools deal with large amounts of dynamic, streaming data and enable real-time understanding and decision-making. However, they still require a significant amount of developer knowledge and skills to operate. A combination of these technologies will enable the creation of new analytic techniques for a responder to develop situational awareness, whether they are in the field or at the command center.

Potential Challenges:

- The ability to validate information from the incident scene in real time can become an issue, particularly if responders will be using this information to inform response operations.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

[69] Soft sensors include data streams that are available to the public (for example, Twitter). Hard sensors include data streams that are not public information (for example, radiological and biological sensor data).

[70] "Infrastructure Protection and Disaster Management Projects," DHS, last updated: December 27, 2012, http://www.dhs.gov/infrastructure-protection-and-disaster-management-projects.

Core Requirements Standard for Response-related Software Applications

Relevance: Responders have multiple concerns about the response-related applications they currently use. For example, they are concerned that the applications may not properly protect their personal information, may not be available at critical times or may not provide technically accurate information. A core requirements standard would create an open standard where developers are able to build applications for the response community that meet a set of minimum requirements. These requirements might include levels of encryption, offline access and verified enrollment, among many others. Development of a core requirements standard would not require all software developers to adhere to the standard, but emergency responders would be aware of which applications did incorporate the standard and could make an informed choice of applications based on this information.

Current Capability: Emergency responders have access to hundreds of software applications, but there is not a core requirement standard that must be incorporated into response-related applications. Essentially, applications are developed by individual entities, and it is the responsibility of the responder to ensure the validity and functionality of actual applications. While responders are experts in their discipline, they may not be able to verify the level of security of these applications or whether they were developed based on the latest science, models and algorithms needed to produce the most accurate information.

Responder Goals:

- Core set of standards that response-related software applications should meet
- Reduces variation between devices
- Standards that address user validation, data standards and validation, functionality validation, operational suitability, ease of use, data security, compatibility and transferability, adaptability for discipline and jurisdictional needs, communication standards and scalability (catastrophic versus daily use)

State of Technology: Requirements standards for applications provide the documentation for developers that govern data outputs (in other words, all measurements must be provided using metric designations). They ensure that data are presented to the user in the format that is expected. The intended audience for an application requirements standard would be the application developer, but the standard would be developed in conjunction with the response community. Such standards are developed routinely and are not technically challenging.

There are several requirements standards pertinent to information exchange that are relevant to the development of an applications standard. The National Information Exchange Model (NIEM) provides a framework for Extensible Markup Language (XML)-based effective and efficient information sharing across all levels of government and private industry. There are multiple schemas within NIEM, especially the support schemas, which apply to application development.[71] In addition, the Unified CAD Functional Requirements document identifies a comprehensive set of functional specifications for CAD systems.[72]

The concept of recognizing components that meet standard requirements is used in other sectors. For example, the DHS SAFETY Act certification and the U.S. Environmental Protection Agency's (EPA) Energy Star designation provide recognition of compliance with standard requirements. Compliance with these standards provides incentives to manufacturers such as protection from liability and the availability of tax incentives for consumers. A similar designation could also be displayed on all response-related applications that follow the standard requirements.

Potential Challenges:

- None identified

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Software Development Kit for Integration of Response-related Software Applications

Relevance: A software development kit (SDK) is a set of software tools that allow for the development of applications for a specific platform or software package. A response-related SDK would be used by software developers tasked to develop applications for the response community. An SDK is necessary to ensure that response-related applications are available on common platforms, as responders do not want an application that is available on only one of the common platforms.

Current Capability: Research and responder input uncovered no known SDK or hosted set of services readily available for the adoption of responder-related applications.

Responder Goals:

- Identifies the necessary and optional common feature sets for response-related applications
- Provides protocols and common features for use of responder-related applications on common platforms

[71] "National Information Exchange Model," National Institutes of Health, last updated: n.d., https://www.niem.gov/Pages/default.aspx.

[72] *Unified CAD Functional Requirements* (APCO International, IJIS Institute, UCAD Project Committee, August 2012), http://www.ijis.org/docs/Unified_CAD_Functional_Requirements_FINAL.pdf.

- Backend that can be leveraged by existing and future responder applications to address common backend functionality (for example, registration, user validation, content security, data sharing)

State of Technology: Developing an application requires four steps. First, a developer identifies the necessary features of the application, commonly called a feature set. Second, software developers code the features. Third, developers expose features that will be seen by the user through APIs. APIs allow a developer to provide functionality to users without giving them full access to information on the application. For example, if an application provides encrypted messaging or a secure login, there is protected information that is not shared with all users. All applications that are developed for use on iPhone, Android and Web-based platforms must adhere to a set of stated requirements. Some of these requirements mandate a certain programming language, while others govern the interface design. These requirements are typically contained in an SDK. In the fourth step, the SDK is built on top of the APIs to ensure that the application can reach the most readily used platforms. An SDK would contain all of the features that responder-related applications should provide.

Backend services support specific user requirements such as registration, content administration and user data-sharing services. Developers of new responder applications currently need to "recreate the wheel" and develop unique solutions to address backend services. For example, each application developer must develop the means to validate whether the user is a responder (or otherwise authorized to use the application). The S&T-funded First Responder Support Tools (FiRST) is one application that provides backend services to support user registration, content administration and user data-sharing services; however, these backend services are not available for use with other applications. Although not technically challenging, there is currently no hosted set of common services that can be adopted by responder-related applications or an SDK to support the adoption of core requirements.

Potential Challenges:

- The appropriate entity to provide responsible ownership and maintenance of an SDK and response-related common services is unknown.

Anticipated Benefits	
Responder Safety	
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Platform for User Evaluation of Response-related Applications

Relevance: Many of the applications developed for responders are tailored to provide specific recommendations or guidelines to improve the safety of responders or the population (for example, bomb standoff distances). It is essential that these applications provide information and outputs that are accurate based on up-to-date science and official operating procedures. These applications also must be tested to perform as designed and function in realistic conditions. User reviews in a traditional app store (or other review forums) are often unregulated where individuals are able to post positive or negative reviews and ratings without verification that they have purchased or used the application. Responders believe the sensitive and critical nature of the response-related applications requires input from verified responder users. Therefore, responders would like a mechanism where they can purchase, rate and review the response-related applications. These reviews could include a standard set of criteria by which applications can be "certified" for use, such as data inputs, content outputs, usability and functionality. Responders desire a combination of a Consumer Reports ™ -style repository with the functionality of a traditional app store in a private forum.

Current Capability: Responders currently purchase applications through traditional app stores or through vendor websites. There is no formalized approach for end-user evaluation of response-related software applications. This is currently done by word of mouth between responders and is very ad hoc. Online forums contain reviews of some applications, and traditional app stores contain reviews and ratings of functionality, but neither the identity of the reviewer nor the verification of purchase is required or available. Some app stores provide verification that the app contains no malicious code, but the validation does not relate to the content or functionality.

Responder Requirements:

- Non-anonymous platform for use review (attributed with name, discipline, rank, location, etc.)
- Includes a mechanism to directly purchase response-related applications
- Compares applications based on qualitative and quantitative factors
- Develops criteria for a "responder-approved" application, including compliance with core requirements and minimum threshold of validated user reviews and ratings
- Designates an entity to issue an "approved" software application list

State of Technology: Private business-to-business (B2B) sites currently exist that restrict the purchase and review of applications to a defined set of users. Subject matter experts who participated in the interview process stated that there are no technical barriers to creating a protected forum for responder review and purchase of applications. The Responder Knowledge Base (RKB) used to provide a forum for users to provide reviews on response-related equipment, but that functionality is no longer available.

Potential Challenges:

- State and local policies may govern the use of certain applications on agency-purchased equipment. Although an important factor in a purchase decision, it is not feasible to capture and maintain information about these policies for all agencies and jurisdictions.

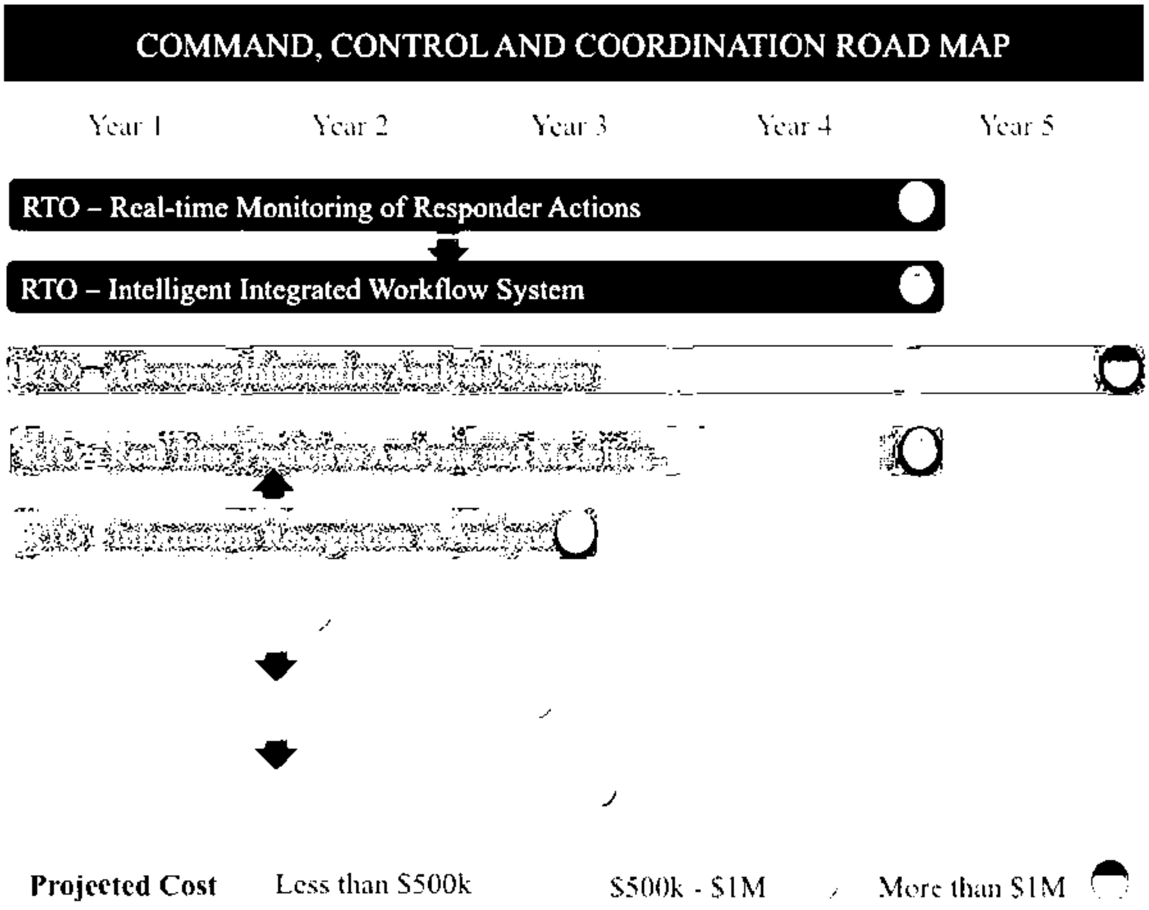
Anticipated Benefits	
Responder Safety	
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

- There are legal liability concerns if user reviews are seen to constitute a recommendation or to represent the opinion of the responder's agency instead of a personal opinion.

Command, Control and Coordination Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the command, control and coordination RTOs above.

- Develop a system to collect automated data and tactical inputs from responders in real time
- Integrate responder geolocation and communication technologies into common operating platforms
- Develop an emergency response workflow of response tasks and objectives
- Develop a workflow system to ingest remote tactical monitoring inputs and customize to execute "intelligent" predictive analysis algorithms
- Establish a program to extract usable data from multiple sources (traditional and nontraditional) and develop machine learning algorithms to produce visualizations of actionable information
- Transition models used in training exercises for rapid deployment and use during response activities
- Develop a platform with integrated sensors and other data streams to collect, mash, analyze and display incident scene information
- Create a requirements standard that defines the format for data and outputs in responder-related applications
- Develop platform-specific SDKs that govern the development of response-related applications
- Create a developer portal with a common backend for user authentication
- Design and manage a forum for review, comparison and purchase of response-related applications


COMMAND, CONTROL AND COORDINATION ROAD MAP
Year 1
Year 2
Year 3
Year 4
Year 5
RTO – Real-time Monitoring of Responder Actions
RTO – Intelligent Integrated Workflow System
Projected Cost
Less than $500k
$500k - $1M
More than $1M

* Core Requirements Standard for Response-related Software Applications

' Software Development Kit for Integration of Response-related Software Applications

• Platform for User Evaluation of Response-related Applications

Figure 17. Command, Control and Coordination Technology Road Map

Responder health, safety and performance is defined as the ability to identify hazards to public safety personnel and develop appropriate mitigations to reduce morbidity and mortality associated with response activities.

There is one capability statement in this domain:

Protective clothing and equipment for all responders that protects against multiple hazards

The purpose of protective clothing and equipment is to shield responders from injury while operating efficiently in hazardous environments and provide the highest level of protection against a range of possible threats.[73] Body protection against individual threats has improved over the last decade; however, it has largely remained limited to the discipline-specific threats that are most likely to be encountered. This stovepiped approach to PPE development and implementation poses several issues. Most notably, responders face a myriad of known and unknown threats during incident response. Therefore, emergency responders often find themselves in situations where they are not outfitted with the best PPE available against the possible range of threats. This approach also does not provide efficient levels of protection across the body and does not allow response agencies to capitalize on economies of scale in purchasing. Responders who participated in PR4 workshops consistently expressed a desire for a modular system built upon a duty uniform that provides limited protection and physiological benefits (for example, moisture wicking) in combination with a series of modular, mission-specific layers to provide specialized protection.

A systems or modular approach allows emergency responders to move beyond a "one size fits all" solution and allows for the customization of their PPE ensemble in varied response environments. This provides several advantages, including preserving comfort and flexibility until the situation demands the next level of protection be employed. This helps ensure that responders are not in the position of choosing between their safety or mission effectiveness. Further, the use of modular layers has the potential to be the most cost-effective option, because only certain layers may become damaged or be in need of decontamination following an incident.

[73] The responders who participated in PR4 focused on body protection from all hazards. However, some reviewers of this document commented that respiratory protection may be more important than protective clothing and ensembles. Respiratory protection (in other words, SCBA, air-purifying respirators, powered air-purifying respirators, escape masks) is not addressed in this document, but has been consistently identified among the priorities in previous Project Responder reports and represents a significant focus of standards and technology development.

Subject matter experts identified five RTOs that correspond with this capability:

- Duty Uniform with Limited Protection Across Threat Spectrum
- Modular Mission-specific Protective Layers
- Wearable Materials and Systems That Can Be Easily Decontaminated
- Wearable Integrated Sensors
- Multi-threat Performance and Testing Standards for a Modular PPE System

Duty Uniform with Limited Protection across Threat Spectrum

Relevance: The duty uniform is the standard clothing ensemble worn by responders on a daily basis. In many cases, particularly for law enforcement officers and emergency medical technicians (EMTs), it may be the only clothing worn while on duty. The development of a PPE duty uniform that provides limited protection against a range of hazards is a well-established need with the emergency responder community. Responders function in unpredictable environments and may encounter threats before they can don the most appropriate PPE. Ideally, the duty uniform should help protect responders against the most likely threats encountered, including fire, blood-borne pathogens, extreme weather and projectiles. Additional layers can subsequently be donned, systematically and incrementally increasing the threat protection for the emergency responder.

Current Capability: While there are variances in color and style among disciplines and agencies, the duty uniform is generally made of cotton, wool or polyester. These uniforms provide little, if any, protection against hazards. For example, EMTs report an increase in Methicillin-resistant Staphylococcus Aureus (MRSA) infections on their knees and elbows from moving bedridden patients. Their duty uniforms provide no barrier against these bacteria. Further, the uniforms themselves could cause additional injury. Responders cited multiple instances where polyester uniforms have melted onto the wearer after being exposed to toxic chemicals or high heat. Duty uniforms in the fire service are often composed, in part, of flame-resistant polymers, which provide some additional protection from thermal, chemical and radiological hazards. Many responders wear a T-shirt and other undergarments under their duty uniform. Some commercially available T-shirts have moisture wicking functionality that helps the responder feel cooler, drier and more comfortable during operations. However, commercially available pieces do not adhere to existing uniform standards.

Responder Goals:

- Integrates into a modular PPE system
- Provides basic protection from most likely encountered threats (for example, fire, blood-borne pathogens, weather extremes, contamination, slashing)
- Provides increased localized protection as needed (for example, knees, forearms)
- Enhances comfort (for example, body temperature regulation, moisture wicking)

- Provides an affordable option that can be utilized across disciplines
- Enhances, does not degrade, responder performance
- Balances wearability, comfort, durability and dexterity
- Accommodates differences in gender and body size
- Able to be laundered repeatedly and frequently
- Ensures visual appearance is still in line with discipline and public image

State of Technology: Efforts are underway to achieve advances in functional design for responder garments. Researchers are developing distributed protection that provides enhancements where most needed (for example, reinforcements to elbow and knee areas), improved placement of pockets and other components to minimize bulk and enhance functionality and the integration of passive and active polymers into the material. Passive polymers are chemical compounds that provide a constant set of properties to the garment and could be applied as a coating to reduce the permeability of the material. Active polymers provide, receive and respond to signals from their environment and could enable a garment to change color based on physical conditions, such as exposure to toxins.

There is no single material that meets all of the goals listed above. However, there are opportunities to integrate innovative materials with improvements in functional design to provide advances that responders are looking for as part of a duty uniform. Unitary knits allow for the construction of garments with no seams or variance in thickness; 3-D weaving allows for lightweight molded and shaped fabric panels that use ultra-high-performance fibers; phase-change materials are able to store or release heat for the wearer; and shape memory alloys expand or contract based on exposure and then return to their original shape when heated.

Potential Challenges:

- Responders rely on the comfort, flexibility and functionality of their duty uniform and do not want these attributes sacrificed for greater levels of protection.
- There is no standard for a modular PPE system, and response agencies may be unwilling to purchase an ensemble that does not meet applicable standards.
- Manufacturers will need to develop training curricula regarding expected levels of protection and limitations of enhanced duty uniforms.
- Some of the modular systems used in other fields are expensive on a per unit basis (in excess of several thousand dollars for standard components). If responder modular components are priced similarly, this could be cost prohibitive for many departments.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	
Multi-incident Utility	❖

Modular Mission-specific Protective Layers

Relevance: Responders don additional garments to protect themselves against specific threats. Firefighters, for example, use an ensemble of a thermal-resistant jacket, pants and boots called "turnout" or "bunker" gear. Many law enforcement officers regularly wear ballistic vests over their duty uniform to protect against projectiles. Responders who participated in the PR4 process consistently expressed a desire for a modular system built upon a duty uniform that would provide limited protection with a series of modular, mission-specific layers.

Current Capability: The current approach to developing and utilizing PPE is highly discipline-specific and is not currently viewed as a systems (or modular) approach. This stovepiped approach to PPE development and implementation poses several issues. Most notably, responders face a myriad of known and unknown threats that may not be within their discipline. This means that emergency responders may find themselves in situations where they are not outfitted with the best possible PPE available against the possible range of threats. In addition, current PPE often unnecessarily exceeds the recommended protection factor, in some areas by 400 percent, while still leaving other areas of the body under-protected. This occurs because of the way in which current PPE is layered, the inability to systematically employ the concept of localized protection and the manner in which PPE is evaluated.

Figure 18. Firefighter Turnout Gear

Localized protection integrates selective areas of the modular PPE in which critical additional protection is most needed. For example, additional localized protection may be added at the arms and chest, rather than the whole garment. Localized protection also includes the selective use of advanced material technologies, such as superhydrophobic finishes. These finishes provide the ability to absorb or draw off liquids, such as sweat. The selective use of localized protection, including advanced material technologies, can dramatically decrease cost and increase wearability.

Currently, PPE evaluation to assess the level of the protection factor is done at the component (individual piece) level. However, there is a need to transition to an approach that produces a modular PPE ensemble that can be holistically evaluated for overall protection. This would enable emergency responders to both understand how they can incrementally increase their protection factors by adding layers and understand the limitations of the PPE.

Responder Goals:

- Integrates into a modular PPE system
- Easily donned and removed

- Includes next-to-skin layers and outer layers to provide varying levels of protection as needed
- Uses a universal interface between layers (in other words, no proprietary interfaces that require responders to purchase all modules from the same manufacturer)
- Enhances comfort (for example, body temperature regulation, moisture wicking)
- Provides an affordable option that can be utilized across disciplines
- Enhances responder performance
- Balances wearability, comfort, durability and dexterity
- Accommodates differences in gender and body size
- Easily maintained, stored and decontaminated, and has a long shelf-life
- Ensures visual appearance corresponds with discipline and public image

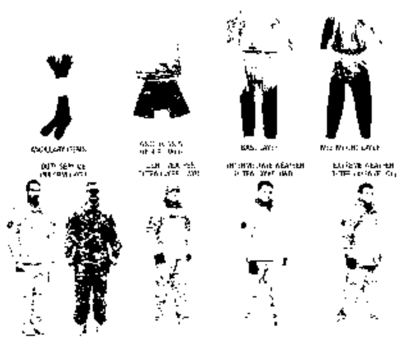


Figure 19. Layers of the ECWCS

State of Technology: Subject matter experts reported that many of the mission-specific garments that responders use are technically mature, with incremental improvements possible to reduce weight and thickness. Advances can be made in the definition and development of a responder-specific modular PPE system. Modular garment systems are generally designed around three primary layers: a base or next-to-skin layer that is designed to wick moisture away from the body; an insulation layer that provides volume and allows warm air to be trapped between the body and the outer garment; and the outer shell layer that protects the wearer from the elements. Additional layers and accessories can be added to increase protection or versatility.

The U.S. Army Natick Soldier Research, Development and Engineering Center (NSRDEC) designed the Extended Climate Warfighter Clothing System (ECWCS) as a modular ensemble for variable combat conditions. Now in its third generation, it includes seven layers of clothing, from lightweight undergarments to extreme cold/wet weather jackets and trousers.[74] The Flame Resistant Environmental Ensemble (FREE) is a PPE system that provides complete fire-resistant protection for the Army. In combination with additional outer layers, it builds on a fire-resistant base layer that provides moisture wicking to ensure comfort and breathability in all climates.[75]

[74] "Extended Climate Warfighter Clothing System," U.S. Army Natick Soldier Research, Development and Engineering Center, http://www.military.com/equipment/extended-climate-warfighter-clothing-system-gen-iii.

[75] "Fire Resistant Environmental Ensemble (FREE)," ADS, http://adsinc.com/equipment/free.

In the commercial arena, multiple manufacturers are developing modular ensembles that allow the wearer to vary his or her level of protection. Advanced hunting apparel, for example, includes a system of multiple pieces that help regulate body temperature, wick moisture, protect against environmental elements and provide insulation. Some of the garments are composed of high-performance layers and membranes that provide liquid barriers and antimicrobial properties. Several of these systems are transitioned from combat gear developed for the U.S. military.

Sporting apparel companies currently produce garments worn next to the skin that provide moisture wicking functionality. These garments help to keep moisture from collecting near the wearer's skin and do not absorb the moisture itself. This helps the wearer feel cooler, drier and more comfortable during physically demanding operations. However, the materials developed for sporting apparel do not adhere to existing uniform standards required for emergency responder PPE.

Potential Challenges:

- Modular layers must be designed to meet operational conditions of the incident scene, which may vary from warfighters to responders.
- There is no standard for a modular PPE system, and response agencies may be unwilling to purchase an ensemble that does not meet applicable standards.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	
Multi-incident Utility	❖

Wearable Materials and Systems That Can Be Easily Decontaminated

Relevance: Each of the response disciplines faces different primary hazards. Law enforcement often responds to clandestine narcotics laboratories; EMS personnel are exposed to a spectrum of biological hazards; hazmat teams face numerous chemical and incendiary threats; and firefighters are exposed to unknown hazards, as they often do not know what is present on the fire ground. During response operations, PPE is exposed to multiple agents, toxins and contaminants, many of which adhere to or absorb into the materials. If the contaminants are not removed, the clothing may pose an ongoing hazard to the responder during later uses. The contaminant and the properties of the garment determine whether the garment can be decontaminated, as well as the correct process to do so.

Current Capability: Decontamination involves in-station laundering or sending the PPE to an alternate site for cleaning. Often, public safety agencies decide to dispose of contaminated items rather than risk additional exposure, despite the high costs of repurchase. This is primarily because they are not familiar with the appropriate decontamination techniques or do not fully trust that the process will keep the responder safe. Determining what type of decontamination strategy to employ is at the agency's discretion and is dependent on its experience and level of risk aversion. This subjectivity can be costly, especially when decisions are made to throw the equipment away or decontaminate them at an off-site location. Responders have limited nondestructive techniques for testing the exposure levels of their PPE. They often are unable to identify all contaminants absorbed into their garments and do not know what decontamination processes are necessary. They also remain uncertain whether decontamination was effective in removing all contaminants. In addition, PPE exposed to certain hazards (for example, asbestos, HIV, MRSA) carry an additional stigma and are more likely to be disposed of, regardless of whether decontamination procedures are available.

Responder Goals:

- Materials that resist absorption of contaminants (for example, coatings)
- Materials that more easily release contaminants
- Materials that indicate the level of contamination
- Garments that can more easily be decontaminated in the station

State of Technology: The potential exists to reduce the contamination on PPE through the application of coatings or treatments during manufacturing. The ability of a liquid to be absorbed into a fabric is dependent on the contact angle of the droplet. Superhydrophobic surfaces resist absorption because the angle created between the surface and the liquid causes droplets to roll off. Superhydrophobic nanoparticles can be applied as a coating to a garment, allowing contaminants to roll off. This creates a self-cleaning property. Use of these finishes in textiles has been demonstrated. The Alinghi sailing team used superhydrophobic jackets that had a microparticle treatment applied during the manufacturing process to increase water repellency during the 2010 America's Cup. Research in this area has primarily focused on absorption of liquids, but Subject matter experts stated that additional work is necessary for particle resistance.

Applying finishes to clothing is an established field, but many advances in this field have not been adapted to responder PPE. Ongoing research is focused on applying advanced textiles to meet responder needs. Recent successes include a hazmat boot made of new textile materials and surface treatments that can be fully decontaminated in the station. The boots are made, in part, of a leather material that repels toxic chemicals. It is possible that finishes could also be reapplied during the decontamination process, actually extending the usable life and protection provided by PPE.

Responders need to understand whether their PPE can be decontaminated for subsequent use or disposed of because the hazards cannot be removed. Responders also need to understand the appropriate methods for decontamination. As stated above, responders believe that they do not have clear guidance about decontamination protocols and procedures. The Technical Support Working Group (TSWG) of the Combating Terrorism Technical Support Office (CTTSO) is currently funding a project to create a decision tool for responders that would enable them to identify the appropriate means for decontamination. This does not address the ability of materials to be decontaminated but should provide advancement in the standardization and reduction of subjectivity in decontamination decisions.

One key factor for this RTO is that there are limited guidelines for maximum skin exposure to contaminants. All current guidelines are based on inhalation exposure. The absence of guidelines results in a de facto "no permissible exposure" limit, despite the fact that the inherent barrier properties of human skin can tolerate much higher concentrations of exposure. DOD has identified skin-exposure levels for chemical and biological warfare agents, but there are no guidelines for emergency response. Subject matter experts reported that compliance with existing standards and guidelines creates a paradigm of providing a greater level of protection than may be necessary, causing trade-offs that reduce comfort, functionality and the ability to decontaminate. They stressed the need for the development of responder-appropriate skin exposure guidelines to facilitate the identification of decontamination protocols for PPE.

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

- The lack of skin exposure guidelines inhibits the development of decontamination protocols that provide appropriate levels of protection for responders.
- The lack of nondestructive sampling techniques prevents responders from being able to identify all hazards present on garments.
- It may be difficult to overcome psychological resistance to wearing garments that were previously contaminated, especially for certain hazards.

Wearable Integrated Sensors

Relevance: Responders experience significant physiological stress during response operations. In addition, they can be exposed to a myriad of hazards. Sensors can be used to monitor responders and relay important physiological and operational data to incident command. Specifically, sensors attached to or carried by responders can provide command with information about their individual health status (for example, responder inactive, physiological factors exceeding set parameters) and specific threats and hazards on the incident scene. Improved awareness of these factors helps incident command make decisions that increase the safety of responders and the population. This RTO focuses on sensors integrated into responder garments or body-worn equipment and does not address hand-held hazard detection devices.

Current Capability: The use of wearable sensors by the response community is limited. Other than specialized units, law enforcement and EMS personnel have no existing sensor systems or physiological monitoring devices integrated into their garments. Most firefighters use a PASS device that provides an audible alert when the firefighter is immobile. The PASS device is integrated into the firefighters' SCBA system.

Other sensors are available, but are not universally used within the fire service, including those capable of monitoring responder heart rate, blood pressure and oxygen levels. Other sensors monitor lack of oxygen, carbon dioxide levels, radiation, temperature and combustible gases. Additionally, there are sensors currently available to monitor general disaster environment elements, such as temperature and smoke presence and position. These sensors often adhere to the outside of responders' PPE. However, sensors that are externally placed are often damaged or rendered unusable during response operations due to the conditions of the response environment. In addition, the sensors do not necessarily provide immediate or actionable information based on the data collected.

Responder Goals:

- Integrates sensors into PPE rather than adhering sensors externally
- Enhances the robustness of sensors, including protection from common threats (for example, chemical, thermal)
- Generates data outputs that provide direct operational relevance
- Provides sufficient SWP without a net increase in the weight of the total PPE ensemble
- Ensures ease in calibration
- Further develops biological hazard detection capability
- Wearable sensors that can be laundered and decontaminated frequently
- Relays information in real time to incident command, caches data when connectivity is offline and automatically forwards when connection is restored

State of Technology: A wearable sensor system has three components: the sensor, the transmission of data measured by the sensor and the display that translates data into actionable information.[76] Many of the sensors identified by the response community have already been developed for other applications. Over the past decade, NASA has been developing and refining the Lifeguard system to monitor the health of astronauts during space flight missions. The Lifeguard system monitors vital signs (in other words, electrocardiogram, temperature, heart rate, respiratory rate, oxygen saturation and blood pressure) and transmits the data wirelessly to a portable base station. Multiple commercial entities are designing and producing compression clothing that has sensors woven into the fabric. These products were initially designed for athletes (for example, a shirt with an integrated bioharness was worn by participants in the 2011 National Football League Combine), but the applications are expanding into other fields.

There are a number of systems in development that are specifically designed to monitor the physiological signs of responders. The Wearable Advanced Sensor Platform (WASP)

[76] "In-Q-Tel Quarterly: What Are Wearables?,,"Zephyr Technology Corporation, last updated: n.d., http://zephyranywhere.com/press/in-q-tel-quarterly-what-are-wearables/.

system includes a flame-resistant T-shirt worn next to the skin. Physiological sensors mounted on an embedded strap track heart rate, heart rate variability, respiration rate, activity levels, posture and other factors. The system transmits data via Bluetooth over commonly used responder radios, cellphones and Wi-Fi networks. There is a portable command station that analyzes the physiological response of individual responders over time. A multi-disciplinary team funded by the U.S. Army NSRDEC is developing WASP.

The Center for Nanotechnology at NASA's Ames Research Center recently developed flexible textiles woven with computer memory. This material could be integrated into a wearable sensor system for the response community, advancing data processing. It could allow sensor readings to be compared with baseline physiological data, allowing for user-specific alerts.

Potential Challenges:

- The FDA regulates sensors that measure some medical data and may have regulatory authority over a wearable sensor system designed for responders.
- The fidelity of physiological measurements is significantly improved when compared with user-specific baseline data. However, it would be a significant and costly effort to gather baseline data on all responders across multiple conditions.
- There may be significant resistance by responders to wearing a device that may cause them to be removed from the incident scene due to physiological measurements.
- The transition from laboratory conditions to real-world operating environments is critical to ensure that accuracy and functionality is maintained.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Multi-threat Performance and Testing Standards for a Modular PPE System

Relevance: A number of performance and testing standards apply to the PPE worn and used by emergency responders. These standards are in place to ensure minimum levels of protection, consistency in performance and uniform testing criteria. Multiple standards development agencies have authored these standards, obtaining input from responders, associations and manufacturers. Response agencies often place greater trust in materials and equipment that meet these standards, and grant funding is often tied to purchasing equipment that complies with applicable standards. In addition, some states have adopted and enforced select PPE standards as law. Responders stated the need for performance and testing standards for a modular PPE ensemble.

Current Capability: No standards currently exist for multi-threat performance and testing of modular PPE system. While performance and testing standards exist for individual items of PPE, there are concerns that some do not reflect actual operational conditions, are not based on performance criteria or do not address technological advancements. The NFPA has two noted standards that relate to body protection for responders, but not necessarily modular PPE: NFPA 1971 and NFPA 1975.[77]

NFPA 1971 is the standard for protective ensembles for structural firefighting and proximity firefighting. This standard "protects firefighting personnel by establishing minimum levels of protection from thermal, physical, environmental, and blood borne pathogen hazards encountered during structural and proximity firefighting operations."[78]

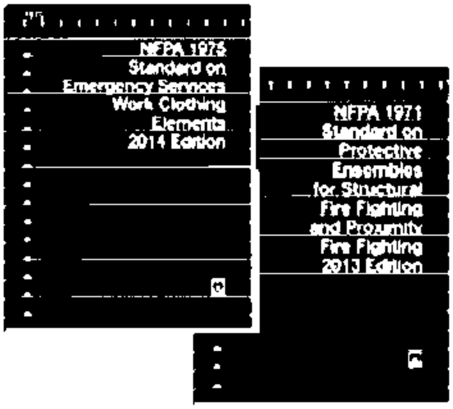

NFPA 1975
Standard on Emergency Services Work Clothing Elements
2014 Edition
NFPA 1971
Standard on Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting
2013 Edition

Figure 20. NFPA Standards Manuals

NFPA 1975 is the standard for station/work uniforms for emergency services. This standard "safeguards emergency services personnel on the job by establishing requirements for flame-resistant station uniform clothing that won't cause or exacerbate burn injury."[79]

Existing standards may not be adaptable to a modular PPE system, however. NFPA 1971, for example, assumes the responder has no garments on below the structural firefighting garments (turnout gear) and does not account for the incremental increases in protection from multiple layers.

Responder Goals:

- Performance and testing standards that account for a modular PPE system
- Common interface for integration of modular PPE component
- Operationally appropriate performance and testing criteria
- Includes recommendations for the retirement of systems

State of Technology: The standards development process and revision cycle do not represent a technical challenge. The design of a modular PPE system and development of prototype ensemble pieces is a prerequisite for the development of this standard.

[77] Two other standards NFPA 1977 (Standard on Protective Clothing and Equipment for Wildland Fire Fighting) and NFPA 1951 (Standard on Protective Ensembles for Technical Rescue Incidents) have some relevance to this RTO, but are not addressed here in detail.

[78] "NFPA 1971: Standard on Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting 2013 Edition," National Fire Protection Association, http://www.nfpa.org/catalog/product.asp?link_type=buy_box&pid=197113&icid=A647.

[79] "NFPA 1975: Standard on Station/Work Uniforms for Emergency Services, 2014 Edition," National Fire Protection Association, http://www.nfpa.org/catalog/product.asp?link_type=buy_box&pid=197514&icid=A647.

Potential Challenges:

- Introducing a new standard can be difficult if there is only one entity producing a prototype because there is limited opportunity for reproducibility of findings or inter-lab testing.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	
Multi-incident Utility	❖

Responder Health, Safety and Performance Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the responder health, safety and performance RTOs above.

- Design a duty uniform that can be used across disciplines and that provides a defined level of protection from identified hazards
- Develop a modular PPE system incorporating next-to-skin layers, duty uniform layers, mission-specific layers and environmental layers that work together
- Develop a cleaning extraction program, initially focusing on a small number of the most common contaminants (six to ten) to evaluate optimal methods for extracting contaminants
- Develop a prototype garment (for example, vest) as a proof of concept for field performance testing and evaluation of wearable integrated sensors
- Develop performance and testing standards for a modular PPE system inclusive of a next-to-skin layer, a duty uniform layer and functional layers

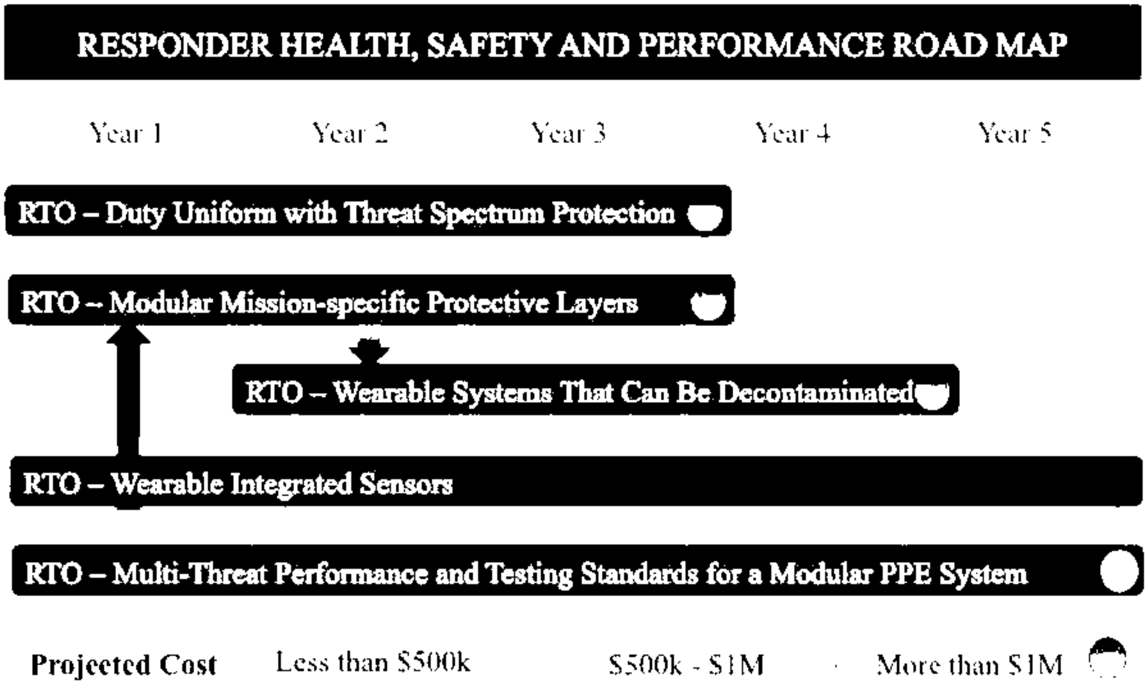

RESPONDER HEALTH, SAFETY AND PERFORMANCE ROAD MAP
Year 1
Year 2
Year 3
Year 4
Year 5
RTO – Duty Uniform with Threat Spectrum Protection
RTO – Modular Mission-specific Protective Layers
RTO – Wearable Systems That Can Be Decontaminated
RTO – Wearable Integrated Sensors
RTO – Multi-Threat Performance and Testing Standards for a Modular PPE System
Projected Cost
Less than $500k
$500k - $1M
More than $1M

Figure 21. Responder Health, Safety and Performance Technology Road Map

Logistics and resource management is defined as the ability to identify, acquire, track and distribute mission-specific equipment, supplies and personnel in support of catastrophic incident response.

There are two capability statements in this domain:

The ability to identify in real time what resources are available to support a response (including resources not traditionally involved in response), what their capabilities are and where they are, in real time

Catastrophic incident response typically involves the participation of a large number of federal, state and local response agencies; National Guard units; volunteer organizations; and private individuals. Each participating party has resources available to it. It is difficult for the logistics section within incident command to understand which resources are needed, which resources are available to meet those needs and the proximity of those resources. Each agency or organization generally maintains a separate list of assets and is not able to readily share resource data with incident command. Additionally, incident managers may have limited information regarding nontraditional or specialized resources that are available or are operating on-scene. Responders would like a logistics management system that allows resource data to be exchanged and provides a clear resource-related common operating picture. This capability need is focused on the availability of resources for response operations.

Subject matter experts identified two RTOs that correspond with this capability:

- Integrated Logistics Management System
- Data Ownership and Exchange Standards

The ability to monitor in real time the status of resources and their functionality in current conditions

Many resources are brought to bear to support incident response operations, including personnel, supplies and equipment needed to stabilize the area, mitigate additional consequences, protect responders and the public and restore the use of critical resources. It is difficult for the logistics section in incident command to understand which resources are on-scene, who is using them, when they need maintenance or rehabilitation, when they are available for subsequent use or tasking and how the resources can be identified and returned to their home agency. Many of the requirements for this capability can be addressed with the development of a resource management system as mentioned above. However, data concerning the functionality of specific resources could improve the incident command's ability to make resource allocation decisions. This capability need is focused on the management of resources already on the incident scene.

Subject matter experts identified one additional RTO that corresponds with this capability:

- Remote Collection of Resource Data

Integrated Logistics Management System

Relevance: Logistics involves the procurement, transportation, storage and maintenance of resources. A logistics management system provides automation and organization of these processes. When applied to catastrophic incident response, it includes tracking the movement of inbound units, ordering new equipment, staging supplies, ensuring the functionality of on-scene equipment and predicting future event needs. Responders would like an integrated logistics management system (ILMS) that illustrates the resources that are available to support a response, the specifications of those resources and where they are located in real time, regardless of the incident's size. They would also like an integrated picture of the status of all resources at the incident scene, regardless of jurisdiction or discipline.

Current Capability: The logistics section is responsible for managing resources during incident response. The logistics section chief and staff are tasked with requesting resources, managing staging and distribution of resources on the scene and maintaining the functionality of those resources. Responding agencies frequently rely on static, outdated spreadsheets to identify the resources available to support a response, making it difficult for the logistics section to develop a clear picture of available resources. In addition, there is inadequate visibility into the status of inbound units or equipment. Responders reported that on-scene staging is frequently ad hoc, with limited predefined organization for placement of resources when they arrive. The use and status of equipment is often managed through paper check-out cards. Sharing resources often relies on having an emergency mutual aid compact in place. It is also difficult to share resource information when the data formats of resource databases are incompatible. The logistics chief can use situational awareness software to request resources and see inventories, but the data cannot be shared with other users to create an integrated picture.

FEMA uses a Logistics Supply Chain Management System (LSCMS) during federal emergencies to track shipments from distribution centers to the federal staging area. A logistics chief places a request into the system, and FEMA supply chain managers validate the order and decide where it will be sourced. If the item needs to be transported from a FEMA warehouse, it is fitted with a GPS transponder that allows the user to track its movement. The logistics chief must place a second order to move the resources from the staging area to the incident scene. At this time, LSCMS cannot be used to track some larger items (for example, vehicles) and is only available to approved users at the state and federal levels.

There are a number of other systems to manage resources on the incident scene, but they are generally task- or region-specific. For example, some jurisdictions use a Medical Emergency Response Center (MERC) to manage the availability of hospital beds and specialized care; the Texas Regional Resource Network (TRRN) was developed for the Governor's Division of Emergency Management to track the state's emergency response-related resources within the state; and the National Wildfire Coordinating Group developed the Resource Ordering and Status System (ROSS) to track all tactical, logistical, service and support resources. All of these systems provide significant improvements in resource management, but the utility and functionality are not universal among response agencies.

Responder Goals:

- Integration of systems to aggregate existing resource information, process resource requests, track the logistics process and record necessary financial information
- Tracks inventory levels, available suppliers and resources, qualified response personnel and transport and distribution information in real time
- Graphic display of real-time resource status at the incident scene (for example, fuel levels, battery life)
- Generates alerts when disposable supplies hit predetermined levels or automatic reordering of supplies given preset parameters
- Models burn rates on a range of resources
- Generates alerts for incompatibility of supply components
- Generates alerts when a resource is scarce on a local, regional or national basis
- Integration of supply chain and product integrity
- Compatibility between incident-related decision support and management systems and financial management requirements or systems
- Resilient stand-alone system that is not reliant on the Internet to function
- Operates using multiple platforms
- Provides visibility of resources at all levels (for example, federal, state, local and private sector)

State of Technology: Commercial logistics management systems address many of the responder goals listed above. These systems focus primarily on supply chain management and provide visibility into the status and transportation of ordered items. Consumers also enjoy advances in this area. As an example, an individual can order, pay for and watch the approach of a requested item (for example, a taxi cab) in real time using an application on his or her smartphone. Much of this utility has not been transitioned to emergency response needs, but several efforts are in development. For example, commercial developers are creating a software application that tracks the movement of inbound personnel. The application can notify a responder that he or she has been activated and can then track inbound movement to the incident scene using cellular and wireless networks.

The National Guard Bureau developed the Civil Support Team Information Management System (CIMS) to coordinate the command and management needs of Civil Support Teams (CSTs). One component of CIMS focuses on logistics. The system is tied to a database of equipment with associated costs. It allows the CST to track individual pieces of equipment by serial number to the user. The system then categorizes the disposition of equipment (for example, lost, returned, damaged, non-recoverable, disposed of) after an incident to support financial accounting. CIMS supports emergency response operations but is not available to the civilian response community.

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

- Entering inventory data is time consuming, and it is difficult to ensure that the information is current. ILMS will not be as useful if the data is not maintained.
- Data and resource typing remains an issue despite expansion of the NIMS classification of types and resources. If agencies do not use the same naming conventions when entering resources into a repository, an integrated system will be less effective in identifying all of the resources available to support the response.

Data Ownership and Exchange Standards

Relevance: Data exchange is the process of sending and receiving data so that the information content or meaning assigned to the data is not altered during the transmission.[80] When large numbers of agencies come together to respond to a catastrophic incident, there is no common picture of the resources available to support response operations. The logistics section relies on inventories provided in multiple data formats, many of which cannot be integrated automatically. In a basic example, two spreadsheets may contain the same types of data, but if the column headings are not the same, merging the data can be problematic. This problem grows in proportion to the number of agencies that arrive to support the response. Data ownership and exchange standards govern how information is distributed and provide a common structure, or schema, so that information contained in the data set can be integrated seamlessly. This will provide the logistics section with a unified picture of all resources available to support the response.

Current Capability: Each response agency maintains its own inventory of assets. This inventory is often recorded in simple spreadsheets or documents. Other agencies enter resource data into commonly used situational awareness software. Some regional entities developed data-sharing protocols for resource data. Additionally, response agencies may

[80] "Data Exchange," Organization for Economic Cooperation and Development, last updated: June 2013, http://stats.oecd.org/glossary/detail.asp?ID=1355.

not be willing to share all of their assets to support the response. An agency may need to retain some assets to cover routine operations, may be unwilling to commit all available assets for fear that the items will not be returned or may want to provide only specific types of resources to the response.

As mentioned in the "Core Requirements Standard for Responder-Related Software Applications" RTO above, there are several requirements standards pertinent to information exchange. That NIEM provides a framework for XML-based effective and efficient information sharing across all levels of government and private industry. In addition, the Unified CAD Functional Requirements document identifies a comprehensive set of functional specifications for CAD systems.

Responder Goals:

- A schema that defines the format and structure for sharing resource data
- Originator of data retains ownership (read-only for users of the data)
- Nonproprietary solutions
- Accommodates different platforms, browsers, combinations and software upgrades
- Addresses firewalls and other network security
- Secure and encrypted system
- Low transition barriers or incentives for participation
- Intuitive to use
- Simple governance structures

State of Technology: The development of data exchange and ownership schema is not technically challenging, and there are multiple examples in the commercial domain as well as the federal government. The U.S. military developed the DOD Architecture Framework (DoDAF) to facilitate information sharing across the department. Within DoDAF, the Meta Model (DM2) provides information needed to collect, organize and store data in a way that is easily understood.[81] The DM2 has three levels: a conceptual data model that defines the high-level data constructs in nontechnical terms; a logical data model (LDM), which adds the technical attributes; and a physical exchange specification (PES) that defines how data will be exchanged.[82] The LDM generates the PES schema definitions in XML, which is a neutral format for sharing data.

[81] "DoD Architecture Framework Version 2.02," U.S. Department of Defense, Chief Information Officer, last updated: n.d., http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework/dodaf20_background.aspx,.

[82] "DoDAF Meta Model (DM2)," U.S. Department of Defense, Chief Information Officer, last updated: n.d., http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework/dodaf20_dm2.aspx.

Through the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, Congress mandated the use of electronic health records (instead of paper records) for medical practitioners who provide Medicare and Medicaid services. In response, health information exchanges have been created to facilitate the secure sharing of electronic patient files. As part of the federal health architecture, the U.S. Department of Health and Human Services developed a Nationwide Health Information Network (NwHIN) that provides common specifications, standards and governance that enable secure health information exchange.[83]

Potential Challenges:

- As mentioned above, some agencies may be unwilling to share resource data in a digital format.
- The cost and complexity of transferring existing resource data into the format governed by the schema may be a significant barrier to transition.

Anticipated Benefits	
Responder Safety	
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Remote Collection of Resource Data

Relevance: The functional status of equipment is an important factor in the success of response operations. Generators may run out of gasoline, chain saw blades become dull or broken, SCBA tanks run out of oxygen and medical treatment supplies are consumed. Responders would like the ability to remotely track on-scene resources for improved situational awareness of the equipment already deployed and its status. Graphically displayed location of resources, status updates and usage alerts can be extremely helpful to inform logistics and resource allocation decisions. This RTO pertains to the equipment used or worn by responders and does not include physiological monitors that measure the health status of personnel.

Current Capability: On-scene resources are generally managed through ICS form 219 (more commonly known as T-cards), which record the status and location of equipment on the incident scene. T-cards include a set of eight status cards that are color-coded based on the type of resource (for example, equipment is recorded on a yellow card, while helicopters are recorded on a blue card). Responders write on the T-card both the time they are checking the equipment in and out and the location they intend to use the resource. The anticipated location of personnel teams or crews is also recorded on T-cards.

Response agencies use dispatch systems to deploy units or response vehicles (commonly called apparatus) to meet response needs. Some systems have the ability to graphically

[83] "Nationwide Health Information Network," HealthIT.gov, last updated: n.d., http://www.healthit.gov/policy-researchers-implementers/nationwide-health-information-network-nwhin.

display the location of a particular apparatus. Responders use ratio relay to verbally communicate resource information and needs from on-scene. Many hospital systems are able to automatically track the use of supplies and automatically order new supplies when inventories are reduced to preset levels.

Responder Goals:

- Identifies resource status (in other words, online, offline, in use, idle), functionality (for example, maintenance requirements, resupply needs) and location (in three dimensions)
- Transmits resource status data to incident command
- Integrates into larger Logistics Management System
- Graphic display of real-time status, functionality and location on a GIS-enabled platform
- Compares resource data against typical, optimal and emergency operating parameters and consumption rates
- Generates alerts when disposable supplies hit predetermined levels and automatic reordering of supplies given preset parameters
- Generates alerts when maintenance and resupply are needed
- Automatic population of financial accounting forms
- Two-way functionality and communication between field and command (in other words, the ability to "command" equipment to reduce consumption rates as necessary)
- Tags or chips attached to equipment should be ruggedized to withstand the heat, humidity, debris or other environmental conditions on an incident scene

State of Technology: Remote site monitoring involves tracking the status of equipment at distant locations. It is done regularly in multiple industries, such as railways and utilities. It is even possible for the manufacturer to remotely diagnose problems occurring in household appliances. Remote site monitoring relies on remote telemetry units (RTUs) that assess functionality, collect system alarms and monitor the environment for critical factors. The data are then aggregated and displayed for the user.

The field of human-machine interface (HMI) design is focused on the interaction between users and mechanical systems. A number of commercially available remote HMI systems are designed to allow users to monitor the status of machines and even control the machine from a smartphone or tablet. These systems use sensor data to provide a graphic display of supply levels, operating parameters and other factors. Although these systems are not focused on response equipment, the technology could be transitioned to meet responder needs.

Fleet tracking and management systems are commercially available that use sensors to track vehicles (using GPS) and report their location, extract vehicle status information, relay maintenance and diagnostic information and transmit alerts and notifications to and from the driver. These systems are in use by some public safety agencies but have not been adopted across the nation.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Potential Challenges:

- A solution to this RTO may present another big data problem as many assets on the incident scene transmit status data in real time.

Logistics and Resource Management Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the logistics and resource management RTOs above.

- Develop a comprehensive public safety logistics management system that addresses resource availability and on-scene resource status
- Develop an open API for the integration of resource data
- Design a standard data collection and transmission HMI appropriate for response resources

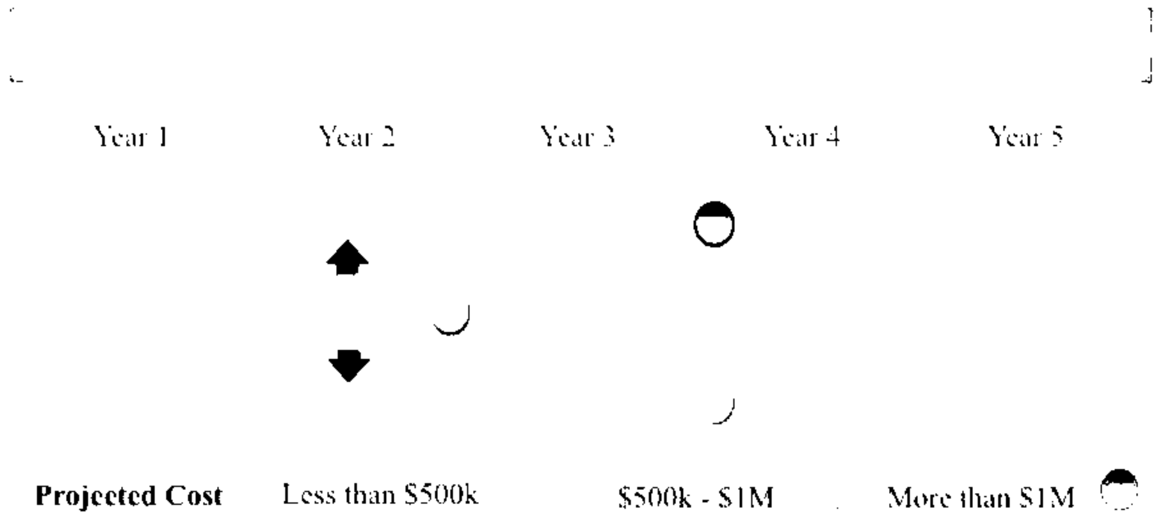


Figure 22. Logistics and Resource Management Technology Road Map

Casualty management is the ability to provide rapid and effective search and rescue, medical response, prophylaxis and decontamination for large numbers of incident casualties and identify appropriate sheltering, transportation and destination options.[84]

There is one capability statement in the casualty management domain:

[redacted]

The purpose of search and rescue is to locate and extricate victims who may be trapped. This mission is primarily achieved by organized search and rescue teams but is also performed by other responders, volunteers or even victims themselves. The search and rescue process can be labor intensive and time consuming, with activities including (1) locating and verifying the presence of a victim; (2) performing necessary stabilization of the surrounding structures or debris; (3) removing the victim; and (4) performing initial medical stabilization efforts. Deceased victims are generally removed following the immediate active search and rescue efforts for living victims.

There are several reasons why responders would like to be able to *remotely* detect the presence of casualties on the incident scene. First, there may be areas that are hazardous for responders to enter (such as a radiological or chemical environment or if a structure is unstable). Incident command would like to confirm the presence of living victims in a geographic area before they deploy their personnel into a potentially dangerous environment. Second, a catastrophic incident scene may be geographically expansive, making it very time consuming to search for individuals in every structure or building. Third, current search and rescue protocols require the location of a victim to be verified by touching or hearing the voice of the individual. Therefore, if a person is unconscious, he or she will not be able to signal to responders. If responders could determine whether there are injured or trapped individuals from a standoff distance, they would be able to locate and rescue victims more quickly, improving their chance of survival. Likewise, responders would be able to more quickly retrieve deceased victims to enable processing (for example, autopsy, identification) and disposition (for example, burial, cremation), as well as decrease health hazards from decomposing remains.

Subject matter experts identified six RTOs that correspond with this capability:

- Remote Sign of Life and Death Detection
- Incident-specific Casualty Modeling and Prediction
- Data Integration and Decision Support for Casualty Detection
- Indoor Casualty Geolocation
- Outdoor Casualty Geolocation
- Subsurface Maritime Casualty Geolocation

[84] A casualty is defined as a person, living or deceased, who has been directly affected by an incident.

Remote Sign of Life and Death Detection

Relevance: A key factor in remotely locating individuals is the ability to detect signs of life (for example, heartbeat, respiration, body heat) or death (for example, gases emitted by decomposing remains). Responders would like positive verification of the existence and location of casualties to improve the efficiency and effectiveness of their search and rescue efforts by focusing on verified locations. They would also like to obtain this verification from a standoff distance to improve the safety of those engaged in the process.

Current Capability: Responders currently use several methods to remotely identify the existence and location of casualties. The options include the use of animals, sensors and camera systems. Animals are primarily used to detect human scent or movement. Dogs are predominantly employed, but others include bees, sea lions and dolphins. Sensors that detect living victims include heat-sensing forward-looking infrared (FLIR) or multi-spectral cameras, ground-penetrating radar (GPR), carbon dioxide detectors and acoustic equipment that can detect signs of life or movement. These sensors are frequently mounted on aircraft, boats, vehicles or robots. Side-scan sonar is used to detect the presence of remains in water. GPR can also be used to detect the presence of remains underground.

Responder Goals:

- Displays the location of signs of life/death on a GIS platform
- Distinguishes between signs of life and signs of decomposition
- Identifies signs of life up to 100 feet below ground
- Differentiates the number of victims in a given location
- Authenticates the identification of victims
- Scalable and adjustable to meet the parameters of the incident scene
- Incorporates survival factors (for example, exposure, dose, weather factors)
- Transmits data in real time

State of Technology: Recent advances have been made in the ability to remotely determine whether living victims are trapped within a structure. As an example, S&T funded the development of the Finding Individuals for Disaster and Emergency Response (FINDER) system. FINDER uses low-power continuous microwave radar technology to detect movements as small as a millimeter within a standing or damaged structure. Algorithms translate this movement to identify respiration and the heartbeat of victims. The system then creates a Keyhole Markup Language (KML) file that can be uploaded to create a GIS display. The equipment is relatively small (approximately the size of a pelican case) and works with a laptop or tablet. Recent tests demonstrated that FINDER was able to locate victims to within five to six feet from a standoff distance of up to 40 feet from the structure. The algorithms can differentiate between human and animal heartbeats and respiration within most parameters.[85] Prototypes of FINDER are currently being tested in the field. This program transitions work completed by NASA's Jet Propulsion Laboratory (JPL) for DOD to detect heartbeats in battlefield applications. In-progress refinements to the system include adding the ability to specify the scan range and working to integrate the device with other platforms, possibly unmanned aerial or ground systems. Additional work is being done to try to identify victims by differentiating between different heartbeat signatures to compare with an exemplar and identify trapped victims.

HSSAI research indicates several approaches are currently being explored to remotely detect the "smell of death." The development of synthetic nose hairs to detect the gases emitted by decomposing bodies and the use of lasers and remote sensing platforms to identify these gases are the subject of ongoing research efforts.

Interview participants also stated that additional advances in remote detection of signs of life or decomposition are possible through the miniaturization of sensors and their integration with small, hand-launched UASs. Efforts to miniaturize sensors are underway for other applications, but Subject matter experts stated they could be easily transitioned to create an integrated standoff system to detect signs of life and decomposition.

Potential Challenges:

- Participants stated there are no technological or regulatory barriers for remote sign-of-life detection.
- Advances in technology may result in changes in tactics, techniques and procedures. Responders may put more faith in current processes that rely on the experience of search personnel.
- UASs need expanded approval by the FAA for increased use in public safety missions.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Incident-specific Casualty Modeling and Prediction

Relevance: To deploy search and rescue personnel more effectively, incident command needs an accurate estimate of how many casualties to expect, the location of the injured and deceased and an estimated time window to rescue a casualty before he or she dies. These projections may be based on various incident-specific variables, including the population of the affected area at the time of the incident (due to variances in population at different times of the day), the size and scope of the incident and the presence of hazards and threats. This information will allow for a more informed requisition and

[85] The FINDER algorithms are able to differentiate between human and animal signatures except in those instances where they are similar. For example, a large dog and a small child have similar heart and respiration rates.

deployment of resources, allocation of victims to functioning health care facilities and establishment of priorities for search and rescue operations.

Current Capability: Tools for casualty modeling and prediction rely heavily on subject matter expertise and census data input. Models and prediction technology are often incident- or domain-specific. For example, there are several models currently employed in the public health arena, including ones that predict the epidemiological impact of communicable diseases. Others provide specific trauma care predictions. Incident-specific modeling exists for weather events (e.g., hurricanes, tornados), which can provide input to casualty-specific modeling tools. Responders also utilize traffic flow and community GIS data when available, although data accuracy is a concern.

Responder Goals:

- Generates probable locations and estimates of casualties based on specific characteristics of the incident
- Integrates information on areas of high-density population in the affected area or path of the incident
- Displays information and analysis on a GIS platform

State of Technology: There are several software applications available to project incident casualties, but they are generally not used by state and local response agencies because of significant training requirements. The Hazard Prediction and Assessment Capability (HPAC) modeling tool, developed by DTRA, models the dispersion of chemical, biological and radiological materials through the atmosphere and predicts casualties based on these calculations. The Consequence Assessment Tool Set (CATS) is another tool that calculates risks to the exposed population using inputs such as HPAC data and other model outputs.

There are other hazard-specific casualty models that can be applied to emergency response. For example, the U.S. Geological Survey developed the Prompt Assessment of Global Earthquakes for Response (PAGER) system that uses global earthquake fatality and loss models to estimate casualties from earthquakes.

Potential Challenges:

- Accurate census data on affected populations at the time of the incident are not always available. Some jurisdictions have overall population estimates for set times throughout the day, but the specificity requested as part of this RTO is not data that are traditionally collected by jurisdictions.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Data Integration and Decision Support for Casualty Detection

Relevance: There are multiple factors that influence the number of persons directly impacted by an incident, including their ability to be rescued, survivability and vulnerability to additional threats. Examples include time of day, weather elements, condition of transportation routes and other critical resources and likelihood of secondary hazards. Incident command needs the ability to integrate available data and information to deploy responders more effectively, including search and rescue teams, to those areas designated as a priority for casualty location and removal. Outputs of this RTO would also allow incident command to equip responders with the appropriate PPE, rescue gear, transportation and evacuation vehicles and medical supplies.

Current Capability: The preponderance of this capability is based on the experience of incident command staff. Responders cited there was no decision support capability focused on casualty detection. Systems exist that provide multi-layer integration of pertinent data, but there are no applications or modules in those systems that focus specifically on casualty detection.

Responder Goals:

- Provides guidance on the location of potential casualties and the resource requirements to remove them from the affected area
- Graphically displays data and recommendations on GIS-enabled maps at a street-level scale
- Integrates key data sources, specifically including:
  - Location of CIKR within the projected area or path (for example, schools, hospitals)
  - Location of known and vulnerable hazards
  - Ongoing community events and activities
  - Location and information about special needs populations (for example, the number of bottled-oxygen-dependent persons)
  - Projected weather forecasts and data
  - Real-time traffic data showing congestion on critical transportation routes
  - Resource availability and specialized capabilities of hospitals and medical centers
- Integrates pre-event and incident-specific risk assessments

State of Technology: Recent efforts to fuse incident-related information have been applied specifically to the integration of search-related data. Using systems transitioned from a DARPA effort to provide information collection and sharing capabilities for warfighters, incident command is able to see the location of all search teams on the incident scene. In the field, teams are able to collect observations and information during the search (in multiple formats, including video files) and the data are visible to all users.

This capability is currently used by the U.S. Army and is being transitioned to public safety missions.

Potential Challenges:

- Data on special needs populations are not centrally collected by most jurisdictions. When collected, the information is not necessarily integrated with electronic situational awareness systems.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Indoor Casualty Geolocation

Relevance: Natural disasters and explosive events can cause extensive damage to structures, trapping people or rendering them incapable of leaving the scene or receiving medical attention. Likewise, chemical or biological events may leave victims incapacitated and unable to help themselves. This RTO is focused on the ability to identify the location of victims in three dimensions inside standing structures and below ground level. A key consideration for this RTO is that the victims are not wearing a tagging device to aid in the identification of their location. The indoor location of casualties is more difficult than the outdoor location, because GPS does not currently function effectively indoors and building materials shield the body from other sensors.

Current Capability: Responders have several options for locating responders inside structures or below ground. As described in the "Remote Sign of Life/Death Detection" RTO, responders use animals and multiple sensor platforms—including multi-spectral and infrared cameras, microphones, radar and sonar—to detect casualties. These sensors can be attached to manned or unmanned platforms. There are commercially available comprehensive systems developed specifically to detect and locate victims inside buildings; however, these systems generally use networked microphones or GPR to detect movement and vibrations of victims. Using this technology is labor intensive and depends heavily on responder experience and expertise.

In some instances, responders have demonstrated the use of smartphone technologies to identify the number or location of victims. Search teams use this technique to "ping" cellphones to obtain a head count of potential casualties or identify approximate locations. This capability is generally available in the short term, as most phones have a 24- to 48-hour battery life.

Responder Goals:

- Precisely locates victims (including latitude, longitude and height or depth) within one foot, up to 100 feet below ground
- Graphically displays data and recommendations on GIS-enabled maps at a street-level scale
- Transmits location data to incident command in real time

- Differentiates between single and multiple individuals, humans and animals, living and deceased
- Locates casualties from a standoff distance
- Includes confidence levels or margin of error (for example, person located at specific coordinates, margin of error within three to five feet)
- Operates continuously for a minimum of 12 to 24 hours

State of Technology: As described above, the S&T-funded FINDER system will allow responders to remotely determine whether living victims are trapped within a structure. Once the technology is commercially licensed and refined, search teams will be able to identify the location of individual physiological indicators within approximately five feet.

The potential exists to locate individuals using components or signals from personal cellphones. Most cellphones, particularly more advanced smartphones, are enabled to transmit a GPS location. Specific applications allow the user, or others, to find the approximate location of the phone as long as the location-tracking feature is on. The phone location is determined via the GPS signal in combination with triangulation data from nearby cellular towers. If these towers are damaged by the incident, or if bandwidth is overloaded by other communications, this capability may be degraded. Geolocation using cellphone tracking is restricted within buildings due to GPS signal blockage and provides limited data on height or depth.

Project Tango, a multi-entity collaboration, may address some of these deficiencies. The goal of Project Tango is to track the 3-D motion of a mobile device. Sensors in the device take millions of measurements each second to create a 3-D map of the space around the user.[86] The system uses simultaneous location and mapping (SLAM) technology originally developed for the U.S. military to track friendly forces. The system has the potential to locate devices enabled with this technology to within centimeters, including height or depth. Subject matter experts who participated in this study stated that phones enabled with this capability may be available in the near term.

Additional advances in this capability can be achieved through the integration of existing sensors onto alternate platforms such as UASs or UGVs. See the "Remote Monitoring of Threats and Hazards" RTO for a detailed description of the use of these platforms for emergency response missions.

[86] "Project Tango," Google, last updated: n.d., https://www.google.com/atap/projecttango/.

Potential Challenges:

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

- Current limitations on the use of UASs and UGVs prevent the deployment of search-related sensors on these platforms.
- The limited functionality of GPS within buildings hinders the use of devices that transmit GPS data.
- The use of personal devices to identify and locate individuals has several challenges. First, recurrent pinging drains the battery on these devices, diminishing the window that they can be used for geolocation. Second, many persons carry multiple devices, which may provide an inaccurate count of potential victims.

Outdoor Casualty Geolocation

Relevance: Casualties may be dispersed across large geographic areas following a catastrophic incident. For example, a tsunami or tornado can disperse casualties over many square miles, and an airline disaster could create a significantly large debris field.[87] Therefore, searchers need to identify the location of casualties across expansive areas and across varied terrain. As with the "Indoor Casualty Geolocation" RTO, the victims are assumed not to be wearing devices that aid in location identification, although personal property (for example, smartphones) may be used for detection. This RTO also addresses the location of casualties on the surface of bodies of water.[88]

Current Capability: Because outdoor geolocation is not bound by the same structural impediments as indoor geolocation, responders have more options at their disposal. In addition to the baseline capabilities used for indoor geolocation, responders may also use aerial line-of-sight searches, sensors (for example, FLIR) attached to airborne platforms and UGVs, satellite and aerial imagery and GPS locators. The technologies used for finding victims on the surface of bodies of water are similar to those for outdoor geolocation on land, although equipment may be mounted on marine vehicles.

Responder Goals:

- Precisely locates victims within one foot

[87] The ground search area for the Columbia space shuttle disaster covered a 25,000-square-mile search area. The terrain of this search area included four national forests, two large bodies of water and large portions of land uninhabited and inaccessible by paved roads. While this is three times larger than most other National Transportation Safety Board investigations, it illustrates the expansive nature of potential search and rescue efforts.

[88] Subsurface casualties are covered in the following RTO: "Subsurface Maritime Casualty Geolocation."

- Graphically displays data and recommendations on GIS-enabled maps at a street-level scale
- Transmits data in real time to incident command
- Differentiates between single or multiple individuals, humans and animals, living and deceased
- Locates casualties from a standoff distance
- Includes confidence levels or margin of error (for example, person located at specific coordinates, margin of error within three to five feet)
- Operates continuously for a minimum of 12 to 24 hours
- Incorporates terrain information

State of Technology: As discussed in the preceding RTO, many of the advances in search technology could result in the integration of sensors with advanced platforms. Subject matter experts interviewed for this study discussed the potential for integrating advanced sensors on UAS and UGVs. For example, Predator-sized UAS fitted with FLIR can be used to search wide areas. However, restrictions on where UAS can fly, the size of UAS used for domestic missions and the design and use of robots and other UGVs hinder advancement in this area.

Responders can use the electronic devices on victims for outdoor location, much more effectively than for indoor location. The transmission of GPS coordinates in cellular telephones, in combination with triangulation of proximity to cellular towers, can provide responders with a more accurate location. This capability can be used to query the cellphones of specific individuals who may be missing or can be targeted across a specific area to determine how many "pings" are returned and therefore approximate the number of victims. Advances in SLAM capabilities will provide significantly more data and could allow geolocation to within centimeters.

Potential Challenges:

- Current limitations on the use of UASs and UGVs prevent the deployment of search-related sensors on these platforms.
- As mentioned in the RTO above, the use of personal devices to identify and locate individuals presents several issues, including battery life and the potential for inaccurate victim counts.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Subsurface Maritime Casualty Geolocation

Relevance: Catastrophic incidents that occur in, over or near water can result in victims being trapped below the surface. Underwater geolocation involves different challenges than location on the surface: water conditions (for example, currents, floating debris) and depth often impair visibility; the survivability of victims is significantly diminished if they are trapped below the surface; water can mask signs of life and decomposition; and flow can transport victims over long distances. This RTO addresses only the location of casualties below the surface of the water.

Current Capability: Specially trained and equipped search and rescue dive teams currently exist to perform this function. Searches are carried out in specific patterns (for example, circular, spiral box). Team members on the surface may help guide the searchers if the water is clear. These teams use a variety of passive and active sonars. Sea mammals such as sea lions and dolphins are occasionally used to assist search and rescue teams. Technology currently used for underwater search and rescue also includes cameras, microphones and self-initiating GPS locators. The U.S. Coast Guard also employs water-current mapping and models using dummies and dye packs to help with underwater searches.

Responder Goals:

- Precisely locate victims within one foot
- Graphically displays data and recommendations on GIS-enabled maps
- Transmits location data to incident command in real time
- Differentiates between single and multiple individuals, humans and animals, living and deceased
- Locates casualties from a standoff distance
- Includes confidence levels or margin of error (for example, person located at specific coordinates, margin of error within three to five feet)

State of Technology: Remotely operated vehicles (ROVs) can conduct underwater searches without endangering the lives of divers. ROVs have multiple applications, primarily for offshore drilling, but the technology has recently adapted to underwater search and rescue. Responders used ROVs to search for victims of the South Korean ferry accident in April 2014.

Potential Challenges:

- Water characteristics (for example, salinity, clarity, wave size) significantly impact the effectiveness of subsurface search efforts. There is limited ability to control these characteristics and improve search conditions.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	

Casualty Management Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the casualty management RTOs above.

- Iterative design improvements for technologies in development and obtain special temporary authorization from the FCC for use of unlicensed spectrum for search and rescue training
- Develop algorithms that model casualty density and locations based on real-time incident data and specific to GIS-correlated segments of the population
- Develop algorithms that produce recommendations for search and rescue priorities and integrate with a comprehensive decision support system
- Continue development of SLAM technology to locate persons using personal hand-held devices
- Continue development of untethered ROV platform and sensor packages

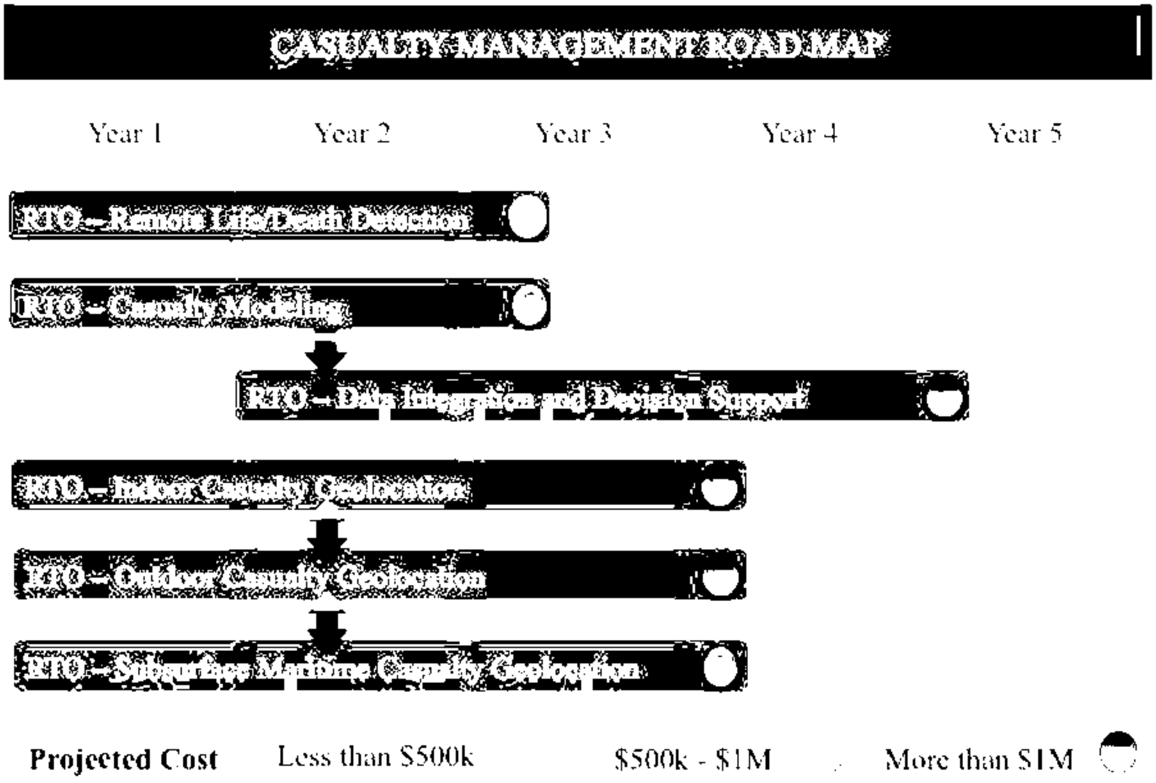

CASUALTY MANAGEMENT ROAD MAP
Year 1
Year 2
Year 3
Year 4
Year 5
RTO – Remote Life/Death Detection
RTO – Casualty Modeling
RTO – Data Integration and Decision Support
RTO – Indoor Casualty Geolocation
RTO – Outdoor Casualty Geolocation
RTO – Subsurface Maritime Casualty Geolocation
Projected Cost
Less than $500k
$500k - $1M
More than $1M

Figure 23. Casualty Management Technology Road Map

Training and exercise is defined as the ability to provide instruction on necessary skills for catastrophic incident response and coordinate and practice the implementation of plans and potential response prior to an incident.

There is one capability statement in this domain:

Readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response

The efficacy of responders is improved through training and exercises. However, training and exercises for response to catastrophic incidents often fail to replicate operational needs and incident effects in a cost-effective manner. Issues with cost, participation and a lack of realism impact the efficiency and effectiveness of the full-scale live exercises held most frequently to prepare for large-scale incidents. Responders would like simulation capabilities that include realistic missions, tools and decision points. Such simulations could allow a large number of responders to train repeatedly and frequently and provide them the opportunity to test their performance in a wide variety of scenarios. Training could be conducted by a variable number of participants, from a single individual to thousands of responders in an agency or region. Virtual training and exercises cannot replace the valuable personal interactions that live training provides for emergency responders. However, virtual training does provide numerous opportunities to significantly reduce infrastructure, equipment and manpower costs and increase responder proficiency.

Subject matter experts identified four RTOs that correspond with this capability:

- Multi-user Virtual Simulation for Training and Exercise
- Artificial Intelligence for Responder Roles and Responsibilities
- Physics-based Operational Elements
- User-specific Simulation Control and Customization

Multi-user Virtual Simulation for Training and Exercise

Relevance: Responders would like high-fidelity virtual simulation tools that allow participants from multiple agencies, disciplines and jurisdictions to train for coordinated incident response. A virtual simulation platform can decrease the costs associated with planning and executing full-scale exercises; increase participation across shifts, stations, agencies, jurisdictions and levels of government; and decrease artificial constraints, such as compressed timetables and always-available resources, that hamper training and exercises today. This RTO is focused on a simulation environment that allows a number of users to engage in scenarios that improve or test the skills needed for emergency response. Other RTOs (see below) address realistic roles and responsibilities, operating conditions and control and customization.

Current Capability: The technology for multi-user virtual training and exercise is readily available through commercial massive multi-player online games. These games provide the immersive environment that responders believe they need, but few systems have been adapted to response needs. Responders cited several platforms currently used for virtual training and simulation. While some provide detailed and highly realistic training and exercise experiences, none provide the ability for geographically dispersed responders to participate in large-scale response scenarios. For example, scenarios may be presented in two dimensions, allowing users to see icons moving on a map, but do not create an immersive experience. Other systems require participants to travel offsite to a central location, limit the number of users or roles or present a limited number of specific scenarios.

Responder Goals:

- Allows single, multiple player and/or massive multiple player interoperability
- Simultaneous and seamless interaction between two or more communities, agencies or entities from dispersed geographic locations
- Nearly real-time, simultaneous interaction between the simulation and all players
- On- and offline capability
- Browser-neutral platform
- Open-source programming
- Scalable virtual space to allow short-duration mini-events through complex incidents
- Low- or no-risk environment for players, creating no public record
- Assesses results against identified scoring or evaluation systems
- Ability to demonstrate and verify competency
- Includes real-time, faster than real-time, fast forward and rewind options
- Includes audio, visual and tactile feedback
- Ability to inject changes into the scenario
- Includes deterministic and stochastic effects
- Includes standardized and user-defined metrics of performance
- Provides opportunity for individual and collective after-action reviews
- Provides in-play trainee feedback

State of Technology: There have been significant advancements in virtual training and exercise over the past several years. Several systems have been developed or transitioned specifically for the emergency response community.

The U.S. Army's Simulation and Training Technology Center (STTC) has extensive experience in the development of advanced simulation-based training for warfighters. DOD's Joint Improvised Explosive Device (IED) Defeat Organization funded an effort known as the Enhanced Dynamic Geo-Social Environment (EDGE) through STTC to train warfighters for counter-IED missions. DHS S&T is now leveraging EDGE to create a simulation platform for emergency responders.[89] The ongoing program recently completed a training platform for law enforcement, EMS, fire, unified command and dispatch to virtually train on a simulated active shooter response. The prototype is built on a well-known game engine that is also used in many consumer first-person shooter and online role-playing games. The goal of the program is to create a customizable, multi-player online game that is interoperable with multiple user interfaces.

DHS also funded a similar effort to develop training for EMS personnel. Zero Hour: America's Medic is a single-player immersive simulation tool for training in triage, treatment, and incident command.[90] Users can choose from multiple scenarios, including mass casualty chemical, biological and explosive incidents and natural disasters.

Several commercial entities also offer emergency response and disaster management virtual training platforms. Currently, providers offer either virtual training at the corporate location or on location in the community. These platforms meet many of the responder goals listed above and offer some capabilities that might enhance an online virtual training and exercise system. For example, some commercial providers include simulator elements, such as vehicle controls, that can enhance the training experience. While much of this virtual training is not within the domain of the online multi-player simulation that responders are looking for, there are multiple components that may be integrated.

Potential Challenges:

- Equipment owned by public safety agencies may be insufficient to run state-of-the art gaming engines. Subject matter experts stated that systems developed for the response community should assume the use of "trailing edge" hardware. Response agencies should not have to purchase new platforms to use the system.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

[89] "Training First Responders for Active Shooter Response," DHS, last updated: November 21, 2013, http://www.dhs.gov/st-snapshot-training-first-responders-active-shooter-response.

[90] "Zero Hour: America's Medic," Applied Research Associates, last updated: n.d., http://www.ara.com/Projects/p_zero_hour.htm.

Artificial Intelligence for Responder Roles and Responsibilities

Relevance: During simulated training and exercises, some of the roles of responders will need to be filled by simulated players. For example, if a single law enforcement agency would like to conduct an exercise, the simulation system will need to replicate the actions of firefighters and EMTs. The decisions and actions of virtual players must mirror those of a real-life responder. Players must be able to interact with simulated responders in the same manner that they do with real participants.

Current Capability: Simulated players are known as non-player characters (NPCs). They are constructed using artificial intelligence (AI) that mirrors the actions and decisions of other players. Commercial online games incorporate highly detailed simulated players, but development of NPCs that mimic responders has been limited.

Responder Goals:

- Ability to create a discipline-specific avatar that can interact with NPCs controlled by AI
- Development of NPCs representative of:
  - Traditional response agencies (fire, law enforcement and EMS)
  - Nontraditional entities (public health, hospital systems and nongovernmental organizations)
  - Hostile forces (for example, an active shooter)
  - Victims and members of the public
- Avatars that accurately represent a gender-specific human form
- Includes physical and mental stressors for players
- Ability for users to play the role of Mother Nature, hostile forces or victims
- Vertical integration and simulation of government roles
- Option for AI to assume role of users who leave the simulation

State of Technology: Subject matter experts report that the development of AI is one of the most complex areas in online simulation and gaming. NPCs have to not only mirror the actions of characters, but also correctly execute a range of decisions. For example, a simulated firefighter must make the same choice as a real firefighter when confronted with the choice between rescuing a baby on the third floor and responding to a fire on the second floor. NPCs that do not act appropriately can degrade the user experience in the training and exercise environment.

The complexity of NPC development depends on several factors. The first is whether the scenario is intended for part-task or full-task training and exercise. It is easier to develop a triage-only NPC for EMT training than one that mirrors the full knowledge and experience of the EMT. The more complex NPC can be used in a wider range of scenarios but is more difficult to develop. The second factor is whether the NPC will be used in a single-player environment or a multi-player environment. NPCs in single-player environments often act as "buddies" who provide advice and recommendations to players. NPCs in multi-player environments play a less prominent role. A third factor is the number of scenarios in the simulation environment. Responders perform different actions depending on the type of incident, which must be mirrored in the development of the NPC. For example, responders don different PPE when responding to a chemical spill than they do when rescuing trapped persons after a building collapse. The NPC must choose the correct actions that correspond with the scenario.

Potential Challenges:

- The level of detail embedded in the AI is a function of cost. Available funding largely dictates the realism that can be portrayed through the NPCs.

Anticipated Benefits	
Responder Safety	❖
Population Safety	
Consequence Mitigation	
Decision Support	❖
Multi-incident Utility	❖

Physics-based Operational Elements

Relevance: The virtual simulation environment must be built on appropriate models to replicate realistic responses and actions. Users will need to identify courses of action, make decisions and act on those decisions within the framework of the scenario. Responders cannot learn from training or exercise if the system does not generate realistic consequences of their actions. For example, virtual triage training for a mass casualty incident will not be effective if simulated victims do not have appropriate physiological responses. The scenario and environment should set the incident conditions to reinforce operational and management skills that will be necessary during a real-life incident response.

Current Capability: Some of the advanced simulation-based training available to responders incorporates physics-based models into the environment (for example, fire and smoke propagation models). In addition, several systems developed for mission-specific training rely on model outputs. For example, simulation-training systems for explosive ordnance disposal (EOD) rely on blast propagation models to govern results within the scenario.

Responder Goals:

- Realistically replicates all elements of incident response
- Realistically represents weather and incident effects
- Accurately portrays virtual objects, characters and environmental effects in three dimensions
- Capability to vary volume levels to reflect cause and proximity of sounds

- Developed with validated physics, chemistry, mathematics and biological models and algorithms
- Ability to input historical data to improve the accuracy of effects

State of Technology: It is possible to incorporate scientific models into simulated training and exercise environments. For example, one developer recently integrated a destruction model, tying the extent of a building collapse in the scenario to variable factors that can be manipulated in the environment. However, many physics-based effects in simulation environments are scripted based on data points and flow charts. For example, the flow rate of water through a fire hose can be accurately depicted in the game without the development of a comprehensive model. The development timetable is increased with the inclusion of physics-based elements. One commercial developer created a fully physics-based gaming system, but it took four years to complete development.

Potential Challenges:

- Coding and design errors in the representation of elements that have a varying value could prove detrimental to the efficacy of the training or exercise. Responders cautioned about the use of models unless validated by Subject matter experts.

Anticipated Benefits	
Responder Safety	❖
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

User-Specific Simulation Control and Customization

Relevance: The utility of virtual training and exercise systems is improved if responders are immersed in an environment that mirrors their own operating conditions. Individual participants, agencies and jurisdictions would like the ability to design and produce operationally realistic scenarios centered on their specific needs. Responders believe they will be better able to prepare for catastrophic incidents if they can use the geography of their own jurisdiction instead of a generic city. For example, a virtual exercise that simulates an explosion at a chemical plant will have a greater impact if responders are familiar with the critical infrastructure (for example, schools, hospitals) in the path of the chemical plume. The ability to customize the training and exercise scenarios will likewise help responders prepare for the incidents that they may be most likely to encounter.

Current Capability: Responders reported that they are largely unable to customize existing virtual training and exercise products. Classroom-based virtual training centers are an exception, as they allow users to choose from a selection of scenarios, environments and objects. There are image libraries of customized towns, municipalities, cities or localities for a limited number of locations that have been designed for large-scale exercises. To date, virtual training and exercise systems have not integrated these images. Existing simulation products generally contain a set number of universal scenarios and offer a geo-typical instead of a geo-specific environment.

Responder Goals:

- Ability for user to design training and exercise scenarios
- Includes geographically correct infrastructure and terrain features derived from GIS data
- Ability to incorporate jurisdiction-specific resources
- Presence of customizable skins (for example, coloring for uniforms, apparatus, buildings)
- Ability to add the location of community-specific known hazards into the virtual environment

State of Technology: Creating a geo-specific location for a virtual simulation requires 3-D digital renderings of the selected infrastructure in that community. It is not technically complex to create a 3-D rendering. One process for creating a rendering is to download street-level imagery, which is readily available online for large parts of the country at no cost. Multiple providers maintain repositories of digital image files for buildings and infrastructure in the United States. As an alternative to downloading imagery, a jurisdiction could purchase or rent a mobile LIDAR platform that could be driven through the community to obtain ground-level images. The USGS produces digital topographic maps of the United States, which are downloadable at no cost and can be integrated into a 3-D rendering of a community.[91] Location-specific images are uploaded to a software program that allows the user to produce a 3-D rendering, complete with accurate placement of exterior details (for example doors, windows). Some systems allow users to include a high-degree of specificity, including the composition of construction materials and the type of window glass on the structure. Some programs also allow users to extend the rendering to include the interior of a structure, allowing specific placement of walls, stairways, doors and even furniture. A jurisdiction can produce 3-D renderings at varying levels of detail.

A level designer integrates digital location data into the engine platform to create a polished visual display. This process is necessary to script how the AI elements will move within the environment.[92] Coding is necessary to define boundaries and movement parameters. For example, characters cannot walk through walls. Systems recently designed for DOD allow some scenario-editing capability, allowing users to define a set of variables, such as the number of players per team or real-time injections of scenario elements. However, the integration of customized or editable locations requires specialized skills.

[91] "The National Map," U.S. Geological Survey, last updated February 27, 2014, http://nationalmap.gov.

[92] A script is a series of instructions written into software code that are used by another software program. The process of writing these instructions is called scripting.

Potential Challenges:

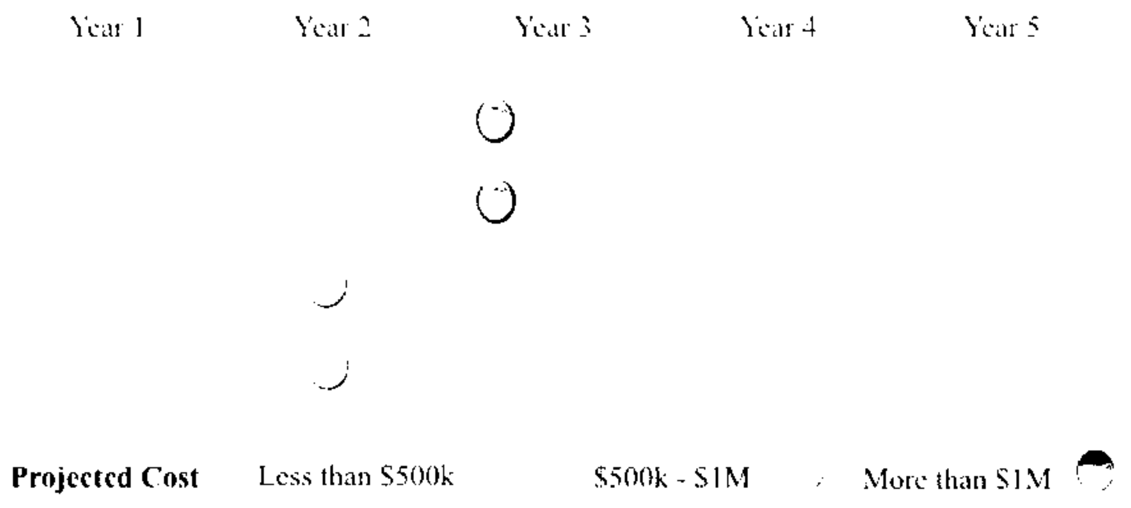
Anticipated Benefits	
Responder Safety	
Population Safety	❖
Consequence Mitigation	❖
Decision Support	❖
Multi-incident Utility	❖

- Each jurisdiction will likely have to bear the costs of creating a 3-D rendering of the infrastructure in its community.
- Although not technically complex, it is time-consuming and expensive to produce 3-D renderings. The combination of cost and duration of the project may limit the scope of the effort.
- Some jurisdictions may be able to afford "boutique" map development, which creates a customized rendering of a specific location within a simulation environment. High costs make this option unaffordable to all but the largest jurisdictions.

Training and Exercise Path Forward:

Subject matter experts identified the following technology programs as necessary to meet some or all of the responder goals listed in the training and exercise RTOs above.

- Continue development of multi-user simulation platform for emergency response-related training and exercises
- Develop an initial set of five NPCs per discipline to perform tasks or provide feedback in a virtual simulation environment
- Identify those elements of the simulation environment that have a varying value
- Develop an integration standard for geospecific 3-D digital renderings



* Physics-based Operational Elements
$^{+}$ User-specific Simulation Control and Customization

Figure 24. Training and Exercise Technology Road Map

CONCLUSION

Technology Plan Summary

This document is the product of the PR4 effort. The purpose of this effort was to examine the state of science and technology for opportunities to address the highest-priority capability needs for emergency response to catastrophic incidents and to develop a plan to address those needs. Two important groups of people made the development of this plan possible.

The first are emergency responders, who respond to catastrophic and routine incidents and who ultimately will use these improved tools, equipment and systems. The responders who participated in PR4 were drawn from traditional and nontraditional public safety disciplines, jurisdictions diverse in size and location and multiple levels of government. The responders identified, described and prioritized the capability needs, and provided qualitative and quantitative goals for needed improvements in those capabilities.

The second group includes Subject matter experts from fields related to the capability needs. Subject matter experts from private industry, academia, federal research agencies and national laboratories participated in the data-gathering efforts. HSSAI spoke with individuals who gave generously of their time to discuss the state of technology and proposed development paths to address responder needs. HSSAI relied on the input and feedback of these groups to ensure that each RTO reflected operational considerations and each was based on an actionable and achievable technology path.

Capability Needs

This document identifies 14 capability needs that responders believe represent the highest priorities for improving their ability to respond to catastrophic incidents. Each of the capability needs may be improved, in whole or in part, through the application of technology solutions. The capability needs include enduring needs identified across the previous phases of Project Responder and emerging needs that will allow responders to leverage technological advances occurring in other fields. Responders prioritized these needs based on their impact on responder safety, population safety, consequence mitigation, decision-making and utility across multiple incidents.

Response Technology Objectives

This plan identifies 42 RTOs that address the PR4 capability needs. The RTOs translate the capability statements into actionable, technology-centric objectives. Each identifies a high-level technology solution (or part of a solution) designed to improve the capabilities of the response community. Each capability need has at least one corresponding RTO, and some RTOs can address multiple needs. The RTO descriptions include projects that represent a proposed path forward for increasing capability. The projects identified in this plan range from short-term initiatives, requiring less than six months of effort, to multi-year research and development programs that may cost tens of millions of dollars.

HSSAI's analysis for PR4 indicates that many of the technologies already exist, though they may need to be customized to meet the operational needs of the response community. Unfortunately, this is not always an easy process. The varying operational environments of responders require tools and equipment that can operate in extreme conditions (for example, high temperatures and humidity, lack of reliable power and communications infrastructure) for extended periods of time. Technologies developed for other fields may need to be reengineered to function in these conditions, which often results in added weight and loss of functionality. In addition, a product designed or redesigned for responders may need to comply with a number of stringent performance and testing standards, some of which should be updated or rewritten to reflect advances in technology.

Key Finding
Many of the potential technology advances will not be possible without the ability to transmit and integrate multiple sources of data. Many of these advances are dependent on sensor systems that provide real-time data about the location of responders, victims, hazards, and resources, the monitoring of physiological data and the progress of activity on the incident scene. Leveraging this technology could significantly improve the safety of responders and the public. However, without a data communications infrastructure, sensors will be able to collect data but may not be able to transmit it to incident command. Further, without a system to integrate the data, decision-makers may not be able to effectively assimilate and understand the large amount of incoming data. For example, the ability to identify the position of a trapped responder in three dimensions, inside a building, is a useful capability only if that data can be quickly and clearly transmitted to the appropriate persons.

Path Forward
Since 2001, the Project Responder initiative has sought to identify and describe the multi-disciplinary capability needs of the response community. This is important because the unique structure of that community significantly influences the technology development and acquisition process. The response community is made up of thousands of career and volunteer agencies from multiple disciplines, each with different priorities and requirements. There is no central coordinating body to gather requirements, obtain economies of scale in procurement, or to fund the development of new capability needs. Since 2003, DHS has sponsored Project Responder to identify the areas where federal investment can make the greatest impact. This plan informs S&T as it makes investment decisions and proceeds with an acquisition strategy designed to address the enduring and emerging emergency response needs. The capability needs and the related RTOs also provide technologists with a vision toward which they can direct their efforts.

The identification of the capability needs and response technology objectives described in this plan are the first steps in providing emergency responders with the capabilities needed to more effectively respond to a catastrophic incident. The responder goals listed in this document provide a high-level overview of what the responders believe is necessary for capability improvement. The projected costs and timetables contained in the technology road maps describe resource requirements at a rough order of magnitude based on those high-level goals. Subject matter experts were hesitant to project time and resource requirements for the potential development programs without a complete description of functional and operational requirements and a defined timetable to meet objectives. For example, identifying overall development costs for an integrated logistics management system is difficult without a detailed understanding of the required inputs and outputs of the system.

There are two primary avenues that DHS can pursue to improve the capabilities of emergency responders based on the information presented in this plan. The first is the development of detailed requirements documents, preferably at the RTO level. The second option is the solicitation of development proposals from private industry, academia and national and federal laboratories that outline their solutions for addressing capability needs.

The first option entails a full requirements-identification process to pinpoint technical specifications. DHS could conduct or sponsor efforts to identify detailed quantitative and qualitative requirements. For example, this process should identify specific thermal loads or water resistance limits articulated by responders. The requirements process should also determine detailed milestones, metrics of success, and costs at a more programmatic level. The output of this process is often called an operational requirements document (ORD). DHS can then solicit proposals to meet the specific requirements described in the ORD.

In the absence of a full requirements analysis, the second option is the development of a statement of objectives (SOO). An SOO is used by DHS to describe a requirement at a higher level than an ORD. The SOO can provide technology developers with sufficient information to allow them to suggest programs that may address responder needs. Developers are not provided with the same depth of information, but are able to propose different solutions to address the capability need. Using the SOO process allows to assess the proposed programs against available budgets to make annual programming decisions.

As technology developers consider responder capability needs, the goals listed in this plan should not be viewed as a set of minimum essential elements that must all be satisfied before new capability is introduced. Responders agree that incremental change through spiral development would provide greater benefit than waiting until all requirements can be satisfied. Finally, technological advances should be integrated, to the extent possible, into all-hazards equipment that is used on a daily basis. Equipment that is used only for responding to and training for catastrophic events may not be used as effectively, if responders are unfamiliar with its operation.

(This page intentionally blank.)

APPENDIX A. PROJECT RESPONDER 2001–2014

The Project Responder effort over the past decade can be divided into four distinct phases. The initial effort, from 2001 to 2004, was funded through a Department of Justice grant to the Oklahoma City National Memorial Institute for the Prevention of Terrorism. The original purpose of Project Responder was to identify operational needs, shortfalls, and priorities for response to catastrophic incidents and develop a technology investment plan to meet identified capability deficits. Shortly after inception, the focus of the effort was fundamentally shifted by the terrorist attacks of September 11, 2001. During development in the initial phase, emergency responders from multiple disciplines and a wide range of jurisdictions and locations participated in a series of interviews and responder workshops. The output of the data-gathering process was the development of a set of 12 capability areas that, as a whole, defined and described the requirements for response to a catastrophic terrorist event. The capability areas were referred to as National Terrorism Response Objectives. Following the identification of capability requirements, a second series of workshops queried technologists from national laboratories, academia and private industry to inform a national agenda for research and development and a corresponding set of road maps detailing new initiative designed to close gaps in emergency response capability.

The second phase of Project Responder was initiated in 2007 by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T). The purpose of the follow-on effort was to examine changes in the emergency response effort since the first report and identify new and enduring capability priorities. Despite the short time frame between the first and second reports, significant shifts in the emergency response mission and needs occurred as a result of an increased focus on "all-hazards" (due in part to events like Hurricanes Katrina and Rita, failure of large-scale infrastructure like the I-35 bridge collapse, pandemic influenza, etc.) and the evolution of national response policy and doctrine with the release of the National Incident Management System and the National Response Plan (which was later revised as the National Response Framework). As a result, the second Project Responder report found significant changes to responder capability needs and related priorities. Emergency responders from a wide range of disciplines, jurisdictions and agencies participated in the effort through a series of interviews and workshops. The findings from the second Project Responder report, released in 2008, included a set of 15 capability priorities and associated challenges in training, technology, management and policy that responders felt constrained the further development of respective capabilities.

In 2011, a third Project Responder effort produced *Project Responder 3: Toward the First Responder of the Future*, examining capabilities needed to fill existing gaps and creating a vision of emergency response in the future. Project Responder 3 was funded by DHS, through a joint relationship between S&T's Support to the Homeland Security Enterprise and First Responders Group and the National Preparedness Directorate of the Federal Emergency Management Agency. In the years since the second Project Responder report was published, a number of economic, technological, infrastructural, and societal developments—as well as a change in the number and type of major incidents facing the nation—combined to change the response environment. DHS believed these changes warranted a reevaluation of capability gaps and resulting investment priorities. As with the two previous iterations, Project Responder 3 used facilitated discussions with a diverse set of responders throughout the United States to identify existing response capability gaps. Through these discussions, participants identified 40 capabilities needed to fill existing gaps. Among these 40 capabilities, responders identified a subset of 12 capabilities as those of the highest importance. Project Responder 3 also produced a compelling vision for potential capabilities that may be required in a future response environment, unconstrained by present-day resource or technical considerations.

PR4 is focused on examining the state of science and technology for opportunities to address the most persistent and highest priority capability needs and developing a plan to address those needs. PR4 continued the interactive discussions with emergency responders and subject matter experts to identify enduring and emerging capability needs; assess the state of science and technology to meet those needs; identify potential technology solutions; and develop road maps that illustrate a coherent technology path to addressing the high-priority needs.

APPENDIX B. PROJECT RESPONDER 4 METHODOLOGY

As described in the body of this plan, the methodology for this effort consisted of data gathering and analysis through four phases:

Phase 1: Identify and Validate Enduring and Emerging Capability Needs
Phase 2: Identify Technology Objectives
Phase 3: Identify Potential Science and Technology Solutions
Phase 4: Develop a Technology Plan and Road Maps

This appendix describes the methodology in greater detail with the goals for each phase, steps within each, and the activities needed to complete those steps.

Phase 1: Identify and Validate Enduring and Emerging Capability Needs

The phase 1 goal was to identify the capability needs that should be addressed in the plan and to validate those needs with a group of emergency responders. Phase 1 was completed using two steps: (1) identification of emerging and enduring needs, and (2) prioritization of capability needs.

For step 1, the Homeland Security Studies and Analysis Institute (HSSAI) facilitated a series of three virtual focus group meetings with emergency responders to determine and validate the set of capability needs to be addressed as part of Project Responder 4 (PR4).[93] The virtual meetings were held over a three-week period in August and September 2013. Participants included more than 75 members of both the First Responder Resource Group (FRRG) and InterAgency Board (IAB). During the virtual meetings, an HSSAI facilitator led participants through a review of the 40 capability needs identified in the Project Responder 3 report and discussed the capability needs that have been consistently rated as a high priority in previous Project Responder efforts. The HSSAI facilitator also asked participants to suggest new or evolving needs that have arisen or increased in priority because of technological advancements, social or cultural changes or other drivers. After analysis of the virtual meeting results, HSSAI identified 14 capability needs for assessment during PR4.

Fiscal considerations dictate that there will never be enough federal funding to address all emergency response capability needs.[94] It is necessary to prioritize among them to identify those where the need is greatest. For PR4, HSSAI wanted to identify those factors that make each capability a priority. HSSAI asked emergency responders from multiple disciplines to identify the factors that cause one capability to be ranked higher than another. The factors that emergency responders consider most heavily when prioritizing capabilities needs include the impact on responder safety, population safety,

[93] Virtual focus group meetings were held using a collaborative web-based system, allowing participants to review materials simultaneously, provide input and feedback verbally and through posted comments.

[94] The first *Project Responder National Technology Plan* identified 84 capability needs, many of which have received little or no funding for development or advancement.

consequence mitigation, decision-making and use across multiple incidents. HSSAI used these factors as the basis to develop an online prioritization tool.

In step 2, HSSAI developed an online tool that responders used to prioritize the PR4 capability needs and invited all members of the FRRG and IAB to participate. Participants rated the 14 PR4 capability needs according to overall priority, the factors identified above and the criticality of need.[95] The prioritization tool was distributed to all members of the FRRG and IAB. It was available over a two-week period. More than 125 responders participated, with a 90 percent response rate for each question.

Phase 2: Identify Technology Objectives

The phase 2 goal was to translate capability needs into technology objectives. Phase 2 entailed three steps: (1) data gathering to better understand the capability needs, (2) facilitation of a focus group meeting to identify draft response technology objectives (RTOs) and (3) facilitation of a workshop to identify responder goals for the RTOs.

It is not sufficient to simply state the emergency response capability needs. Without additional information, technology developers cannot move forward to make advancements. They need to understand the actual capability gaps—the difference between current capability and what responders believe is required to properly and successfully complete their tasks and mission. This requires a clear articulation of baseline capability—what responders have now—and quantitative and qualitative goals that describe what they believe is needed. In step 1 of phase 2, HSSAI facilitated discussions with members of the IAB's Strategic Planning Subgroup to gather initial data on baseline capabilities. Participants reviewed the 14 PR4 capability needs and provided information and data about their current capabilities (technology, policy, procedure and training) available for response operations.

RTOs translate responder capability needs into technology-centric objectives. In other words, an RTO should identify a high-level technology solution (or part of a solution) for a capability need. To develop the RTOs (step 2 of phase 2), HSSAI facilitated a focus group meeting in November 2013 between emergency responders with experience in catastrophic incident response and recognized technical subject matter experts in fields related to the capability needs. The purpose of the focus group was to identify the RTOs that correspond with the PR4 capability needs identified during phase 1. The HSSAI facilitator asked responders to describe each capability need in detail, explaining the operational issues that they face. Subject matter experts then translated those needs into technology objectives. The Subject matter experts identified 58 draft RTOs that correspond with the 14 PR4 capability needs during the focus group meeting.

It is difficult for Subject matter experts to identify a proposed path for improving capability unless they have a clear understanding of what the responders believe is needed. In March 2014 during step 3 of phase 2, HSSAI facilitated a workshop with 26 emergency responders. The workshop's purpose was for participants to characterize the tools they currently have available and to identify goals for each of the RTOs. HSSAI

[95] See Appendix C for a more detailed discussion of the PR4 prioritization process.

facilitators led participants through a detailed discussion of each RTO, asking them to comment on current capabilities, identify qualitative and quantitative goals and discuss potential challenges that might hinder development or adoption of new technologies. HSSAI invited participants from multiple disciplines, areas of the country and levels of government to obtain diverse points of view.

Phase 3: Identify Potential Science and Technology Solutions

The phase 3 goal was to evaluate the state of science and technology to identify potential technology solutions that meet responder needs. Phase 3 consisted of two steps: (1) data gathering and research on the technologies associated with the RTOs and (2) interviews with Subject matter experts.

Some RTOs require advancements in basic and applied research. Some RTOs necessitate new or continued development of existing technology programs, while others need only the transition of existing technology to the responder applications. In step 1 of phase 3, HSSAI researched the state of technology associated with the 58 RTOs to identify the use of similar technology in unrelated fields as well as ongoing research and development efforts. HSSAI analysts reviewed open source websites, publications, technical journals, conference proceedings, and other relevant sources. The purpose of this research was to provide contextual descriptions of the related technology and to identify Subject matter experts for the subsequent interview process.

In step 2, HSSAI engaged Subject matter experts from the national laboratories, academia, and private industry to provide input about each technology objective and to identify quantifiable development requirements. During a series of in-person and telephonic interviews, HSSAI asked the Subject matter experts to propose potential solutions for each RTO. In addition, HSSAI asked them to discuss anticipated costs and timelines and anticipated risks and challenges for the potential technology solutions. Subject matter experts were selected based on several factors including real-world experience, academic background, publishing credits and overall recognition within the domain. Based on the input of the Subject matter experts that some of the RTOs did not entail technology solutions, HSSAI reduced the number of RTOs from 58 to 42.

Phase 4: Develop a Technology Plan and Associated Road Maps

The goal of phase 4 was to assess and integrate the information from responders and Subject matter experts to identify actionable programs for increasing capability. Phase 4 entailed two steps: (1) characterization of proposed technology paths designed to improve capabilities, and (2) development of consolidated technology road maps within each domain.

In step 1 of phase 4, HSSAI assembled the inputs from the Subject matter experts and developed a coherent description of each RTO. Each RTO was described in terms of:

- Relevance: why advancements in the technology objective are necessary, including information on baseline capabilities and why the capabilities are currently insufficient;

- A program description: including the goals articulated by the responders during the workshop and a proposed path to achieve those goals based on the technologists' input; and
- State of technology: a description of the current maturity of the technology (in use and in development) and potential technology barriers that may inhibit further advancement.

In step 2 of phase 4, HSSAI developed a series of road maps that illustrate the projected timetables and estimated costs for each RTO. The road maps include new or transitioned technologies and knowledge products that can result in a measurable improvement in capability. HSSAI created one comprehensive road map for each domain.

HSSAI distributed a draft of the road map to and solicited comments and suggested edits from the FRG and all responders and Subject matter experts who participated in this effort. To the extent possible, HSSAI incorporated this feedback into the final version of this plan.

APPENDIX C. PROJECT RESPONDER 4 PRIORITIZATION PROCESS AND RESULTS

In previous iterations of Project Responder, participants engaged in workshops to identify needed response capabilities and prioritize their importance. This approach was ideal because it provided a logical path to (1) learn what responders believe to be critical gaps in their ability to respond to catastrophic incidents, (2) identify specific capabilities required to meet these needs, and (3) prioritize these capability needs according to how urgent and important they are.

The Q methodology was well suited to rank order the large number of capabilities in previous Project Responder iterations. However, this technique is not suitable for understanding the underlying factors necessary to prioritize a small subset of enduring and emerging capability needs. The Homeland Security Studies and Analysis Institute (HSSAI) worked with survey experts to develop a uniform prioritization tool that is tailored to the subset of Project Responder 4 (PR4) capability needs. This approach analyzes specific factors that make each capability a priority. Knowing these factors will help guide investments to meet the highest-priority needs and improve catastrophic incident response.

This appendix provides a detailed discussion of the developmental steps and the implementation of the PR4 prioritization process.

Methodology

The prioritization process is a uniform method that emergency responders used to prioritize the PR4 capability needs. This process was developed and implemented using a four-step methodology, including (1) identification of prioritization variables, (2) development of a question set, (3) design of an online tool and (4) distribution and data collection.

Step 1: Identification of prioritization variables

To identify the factors that emergency responders use when ranking capability statements, HSSAI interviewed a group of responders from multiple response disciplines. Each responder was interviewed by telephone and asked to identify the factors he or she would consider when assessing the relative importance of a capability. To assist in the process, HSSAI used a small sample of capability statements to extract recurring factors in a consistent manner.[96] Responders were specifically asked to consider the sample

[96] Sample capability statements used to extract prioritization factors during the interviews include: 1) The ability to know the location of responders and their proximity to risks and hazards in real time; 2) The ability to identify what resources are available to support a response (including resources not traditionally involved in response), what their capabilities are and where they are, in real time; 3) The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground); and 4) The ability to remotely scan an incident scene for signs of life and decomposition to identify and locate casualties and fatalities.

capability statements to determine “what makes this capability a priority” and “what specific factors are considered when making this capability a priority.”

Responders identified six overarching variables that are considered when denoting a capability need as a priority. They stated that a capability would be prioritized higher if it accomplished one of the following:

1. Increased responder safety;
2. Increased the safety of the affected population;
3. Mitigated incident consequences;
4. Informed decision-making for incident management;
5. Improved the response for various types of incidents; or
6. Impacted the overall effectiveness or efficiency of the response.

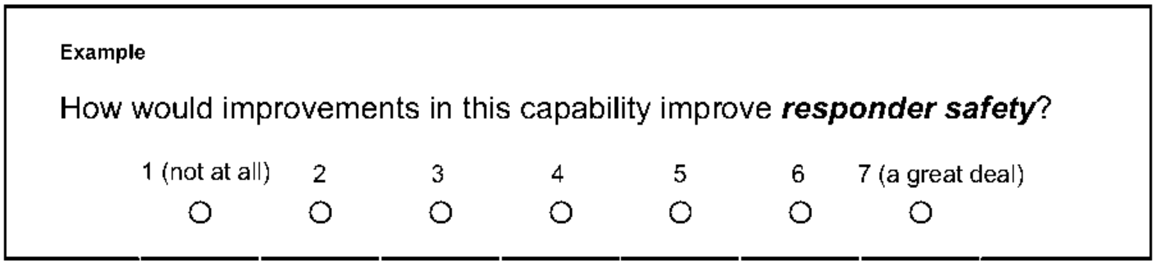
Step 2: Question set development
The study team worked with a subject matter expert to develop a question set that would elicit the necessary information to prioritize the capability needs. The final question set included a series of questions for each capability to determine what makes it a priority. Participants were asked to rank each answer on a scale from 1 (lowest) to 7 (highest).

- How would improvements in this capability improve responder safety?
- How would improvements in this capability improve the safety of the affected population?
- How would improvements in this capability improve the ability to mitigate incident consequences?
- How would improvements in this capability improve decision-making for incident management?
- Can improvements in this capability be used in multiple types of incidents?
- Overall, how important a priority is this capability?

Responders were also asked to rank what they perceive to be the top three (in other words, most important) capability needs and the least critical capability need. Because priorities are subjective, HSSAI also developed questions to identify the discipline, level of government and jurisdiction of the participant.

Step 3: Online tool design
To conduct the assessment, the study team identified a customizable, online tool to walk responders through a uniform assessment of each capability statement. HSSAI used a research suite from Qualtrics.com that enabled the collection and analysis of responder provided data.

For each capability statement the tool provided a seven-point, Likert-style scale, with 7 representing the highest level of improvement for each priority. Below is an example of how the questions were presented to the responders.



Example

How would improvements in this capability improve ***responder safety***?

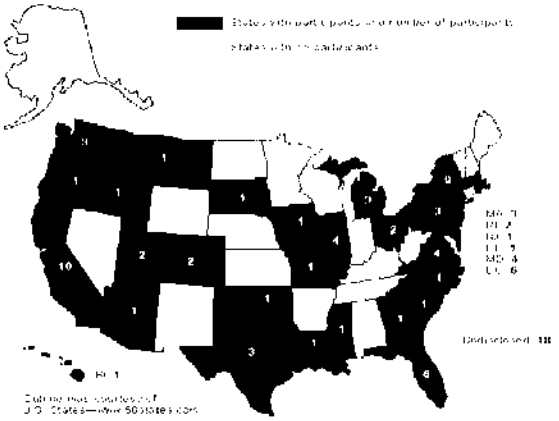
1 (not at all)	2	3	4	5	6	7 (a great deal)
○	○	○	○	○	○	○

Figure 25. Sample Question From Prioritization Process

Step 4: Distribution and data collection

HSSAI invited all members of the First Responder Resource Group (FRRG) and InterAgency Board (IAB) to prioritize the PR4 capability statements using the online tool. FRRG and IAB members received a link to access the tool. The prioritization tool was available from September 25 through October 7, 2013. A total of 135 emergency responders participated in the prioritization process.[97]

Responders from 31 states and multiple disciplines participated in the prioritization process.



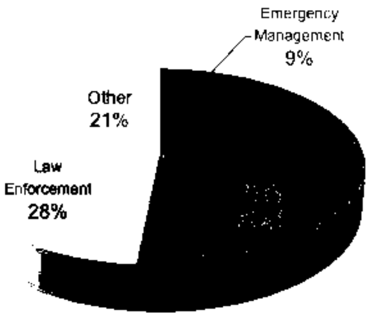


Figure 26. Prioritization Participation by State

Figure 27. Prioritization Participation by Discipline

Results

The total mean score was collected for each of the questions in the prioritization process and analyzed by HSSAI.[98] The prioritization process results can be depicted in many

[97] Although there were 135 participants, not all completed the prioritization process. Each question received between 117 and 128 responses (an average response rate of more than 90 percent). In total, 129 individuals completed the entire process.

[98] For the purposes of this study, the mean score is the average score of all the responses for a specific question.

different ways. The following sections are select tables and visual representations of the data that best reflect the objectives of this study.

The following table represents the top capabilities, based on the mean score of the combined responses to the priority questions for each capability statement.

Capability Need	Mean Score
The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)	6.3
The ability to know the location of responders and their proximity to risks and hazards in real time	6.1
The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time	6.0
The ability to rapidly identify hazardous agents and contaminants	5.9
The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time	5.7
Protective clothing and equipment for all responders that protects against multiple hazards	5.4

Figure 28. Top Capability Needs Based on "Overall Priority"

Responders were asked to rank each capability need on a scale of 1 to 7; a ranking of 7 meant that achieving this capability would be the largest improvement to "overall impact" of a responder's ability to perform his or her job during a catastrophic incident. Figure 28 shows the top capability needs based on the overall mean score (in other words, combined average) for the responses to this question.

Most responders rated the following capability as having the greatest "overall impact" on their ability to respond to incidents.

- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)

Capability in Rank Order	Priority Areas				
	RS	PS	MIC	DIM	CC
The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground	6.6	5.68	6.13	6.24	6.34
The ability to rapidly identify hazardous agents and contaminants	6.24	6.13	6.02	6.08	5.62

RS= Responder safety
PS= Population safety
MIC= Mitigate incident consequences

DIM= Decision-making for incident management
CC= Crosscutting capability
= Highest mean score for priority area

Figure 29. Top Capability Needs Per Variable

The mean scores shown in figure 29 provide additional insight as to why each of the top capability needs is a priority. The following are the top three results for each priority area.

Most likely to improve **responder safety** during a catastrophic incident:

- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)
- The ability to know the location of responders and their proximity to risks and hazards in real time
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time

Most likely to improve **population safety** during a catastrophic incident:

- The ability to rapidly identify hazardous agents and contaminants
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time
- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)

Most likely to **mitigate consequences** during a catastrophic incident:

- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)
- The ability to rapidly identify hazardous agents and contaminants
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time

Most likely to improve **decision-making for incident management** during a catastrophic incident:

- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time
- The ability to know the location of responders and their proximity to risks and hazards in real time

Most likely to **apply to multiple incident types** for catastrophic incident response:

- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)
- The ability to know the location of responders and their proximity to risks and hazards in real time
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time

Additional metadata was collected for each participant, including his or her agency's city and state, level of government and emergency response discipline. Using specific metadata, such as response discipline, HSSAI was able to determine which disciplines ranked which capability needs highest. For example, the ability to know the location of responders and their proximity to risks and hazards in real time ranked highest among firefighters. The ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into operations ranked higher among law enforcement personnel.

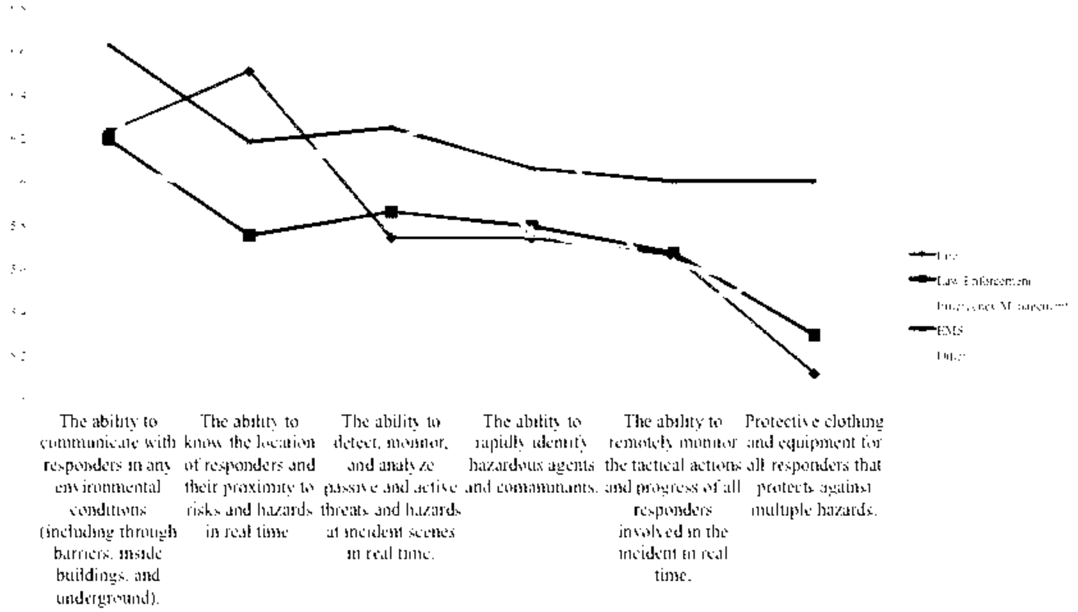


Figure 30. Top Capability Need by Discipline

Figure 30 shows how each discipline scored the top capability needs on a scale of 1 to 7. Each score depicted in the graphic is an average of the total responses from each discipline category for the top capability needs that would make the greatest impact on the overall response to a catastrophic incident.[99]

Top 3 Most Critical Capabilities	1	2	3	Total Votes
The ability to know the location of responders and their proximity to risks and hazards in real time	47	22	16	85
The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)	28	22	20	70
The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time	12	16	11	39
The ability to rapidly identify hazardous agents and contaminants	5	11	11	27
Protective clothing and equipment for all responders that protects against multiple hazards	7	9	4	20
Communications systems that are hands-free, ergonomically-optimized and can be integrated into personal protective equipment	2	10	6	18
The ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into incident command operations	4	7	6	17
The ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time	3	3	11	17
The ability to remotely scan an incident scene for signs of life and decomposition to identify and locate casualties and fatalities	1	5	10	16
The ability to identify in real time what resources are available to support a response (including resources not traditionally involved in response), what their capabilities are and where they are, in real time	1	5	9	15
Readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response	4	5	4	13
The ability to identify trends, patterns and important content from large volumes of information from multiple sources (including nontraditional sources) to support incident decision-making	2	4	6	12

[99] The 'other' discipline category consists of either retired, homeland security, federal agency or other emergency response professionals who are not affiliated with any of the other four categories (fire, law enforcement, emergency management and emergency medical services).

Top 3 Most Critical Capabilities	1	2	3	Total Votes
The ability to monitor in real time the status of resources and their functionality in current conditions	3	1	4	8
The ability to identify, assess and validate emergency-response-related software applications	2	0	0	2

Figure 31. Most Critical Capabilities

Participants were asked to consider all capability needs and rank the top three they felt were the most critical to achieve advances for catastrophic incident response. Participants selected a capability that was the single most (column 1), second most (column 2), and third most (column 3) critical. Figure 31 represents the responses ranked in order by the highest total votes per capability.

The following capabilities ranked the highest in order of votes for the single most critical capability need to address (column 1) as well as total number of votes for being either the first, second, or third most critical capability need:

- The ability to know the location of responders and their proximity to risks and hazards in real time
- The ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)
- The ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time

Least Critical Capabilities	Votes	%
The ability to identify, assess and validate emergency-response-related software applications	70	59%
The ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into incident command operations	10	9%
The ability to remotely scan an incident scene for signs of life and decomposition to identify and locate casualties and fatalities	9	8%

Figure 32. Least Critical Capability Needs

There is no doubt that all 14 capability needs are high priorities to the emergency response community; however, HSSAI asked participants to select the one capability they would consider being the least critical of the 14. Figure 32 shows three capabilities that were rated as least critical.

The majority of participants (59 percent) considered the following capability to be the least critical of the 14 capabilities:

- The ability to identify, assess and validate emergency response-related software applications

The following section examines each capability need independently and shows results using the mean score based on the seven-point scale for each variable.

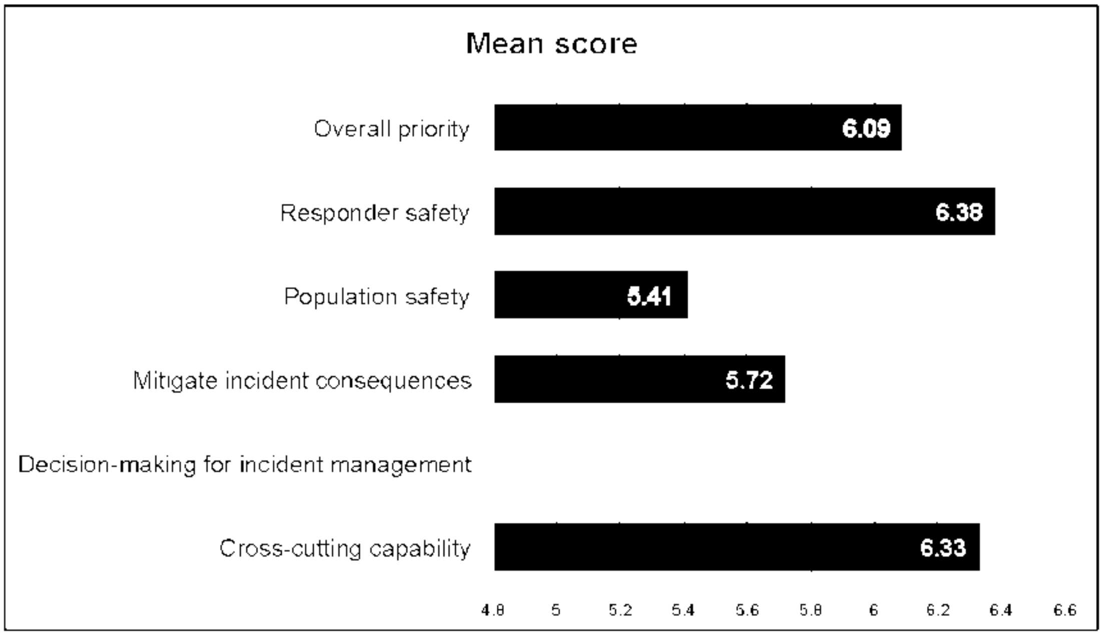


Figure 33. Mean Scores: ***ability to know the location of responders and their proximity to risks and hazards in real time***

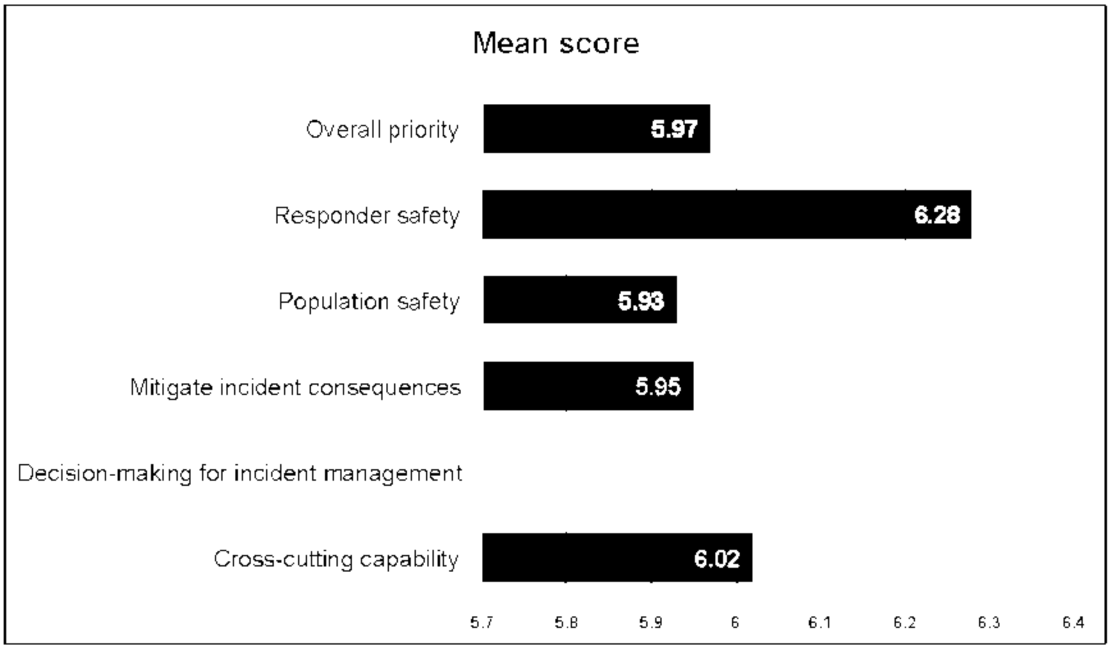


Figure 34. Mean Scores: ***ability to detect, monitor and analyze passive and active threats and hazards at incident scenes in real time***

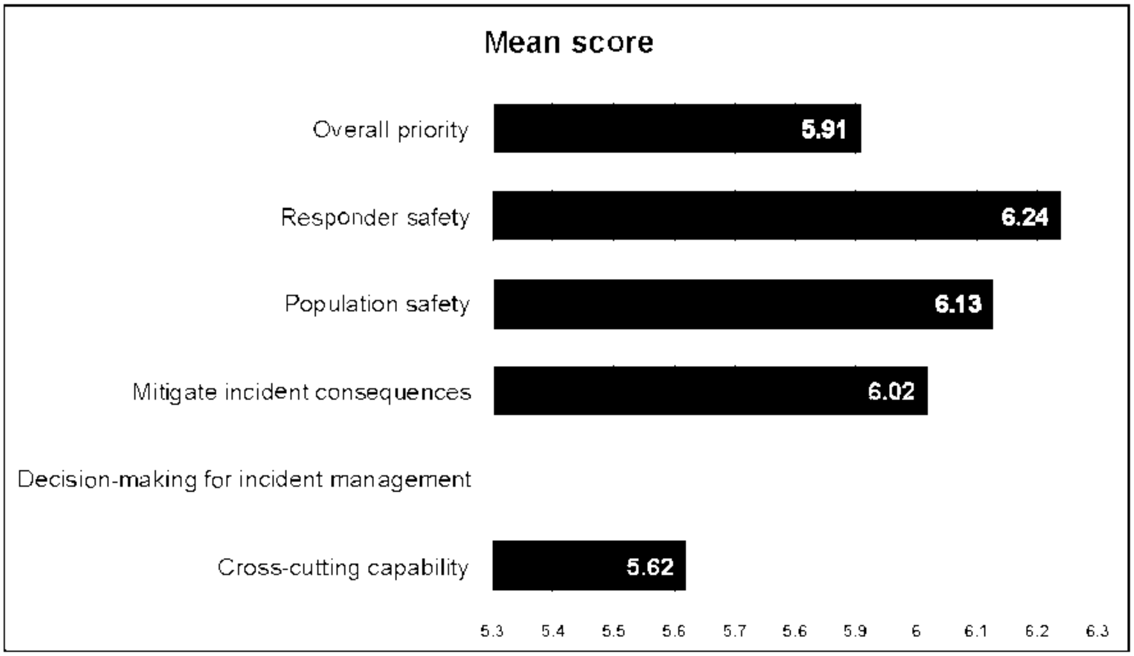


Figure 35. Mean Scores: ***ability to rapidly identify hazardous agents and contaminants***

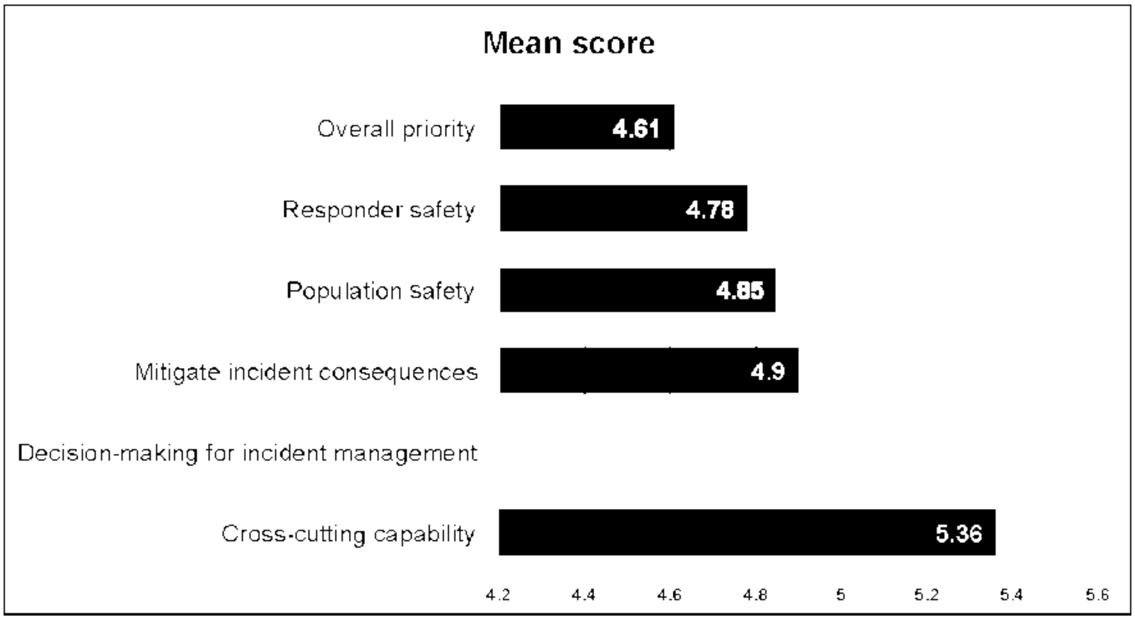


Figure 36. Mean Scores: ***ability to incorporate information from multiple and nontraditional sources (for example, crowdsourcing and social media) into incident command and operations***

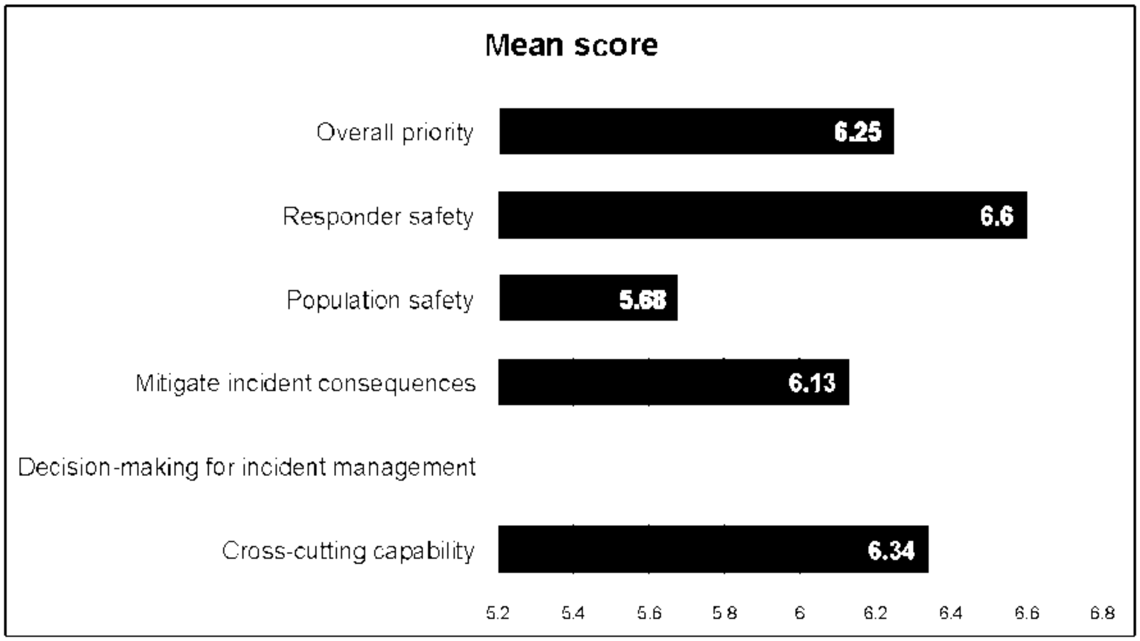


Figure 37. Mean Scores: ***ability to communicate with responders in any environmental conditions (including through barriers, inside buildings and underground)***

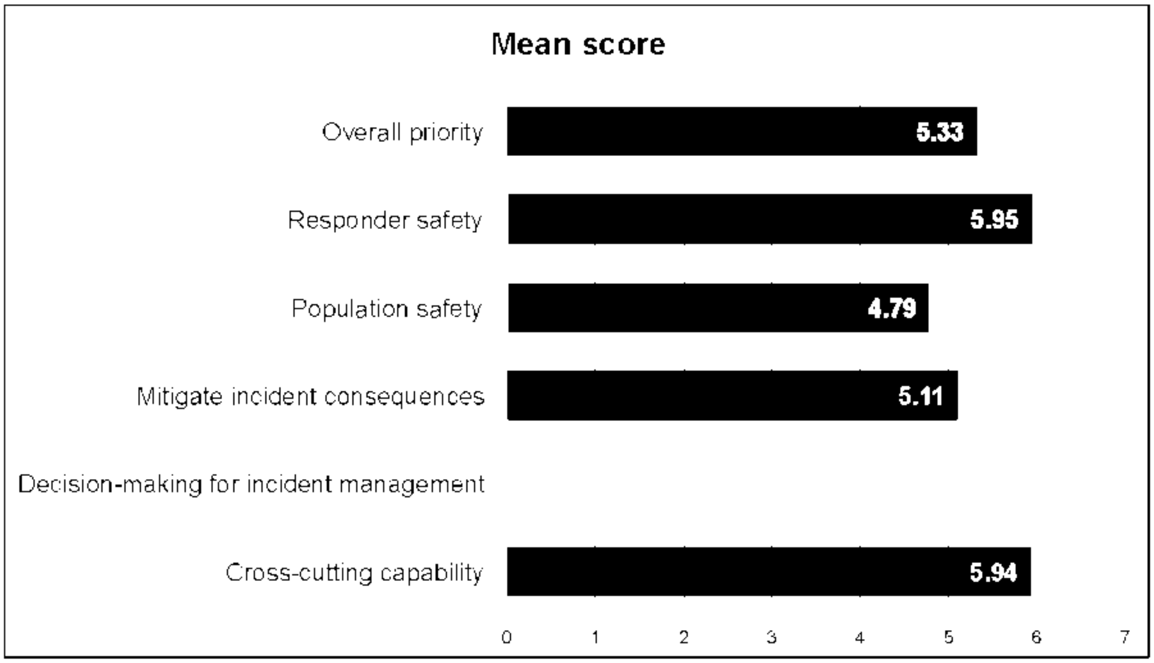


Figure 38. Mean Scores: ***communications systems that are hands-free, ergonomically optimized and can be integrated into personal protective equipment***

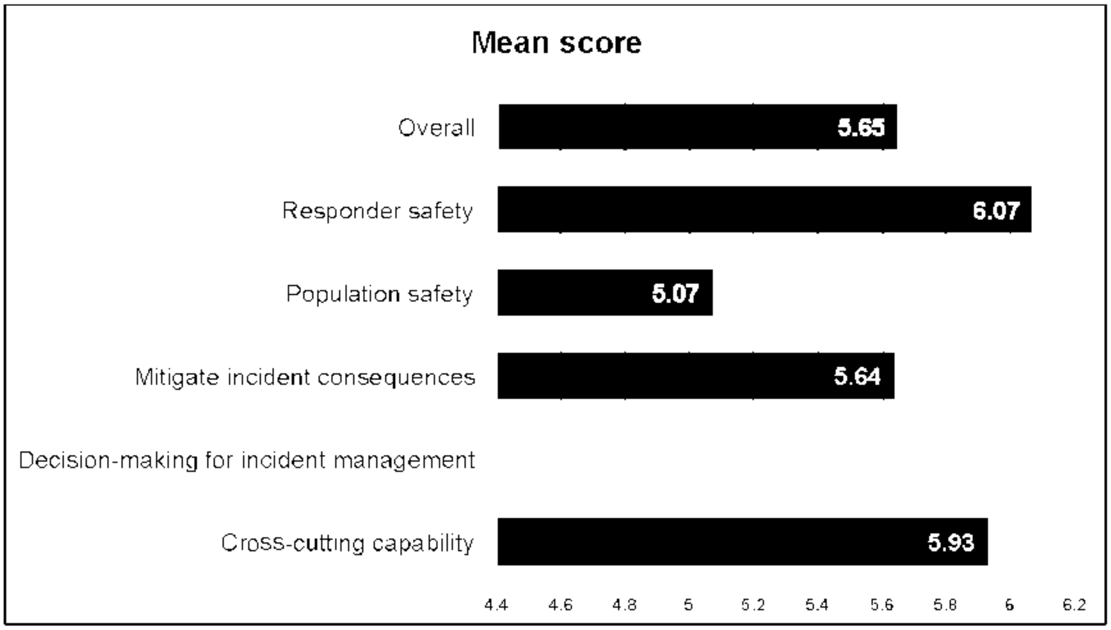


Figure 39. Mean Scores: ***ability to remotely monitor the tactical actions and progress of all responders involved in the incident in real time***

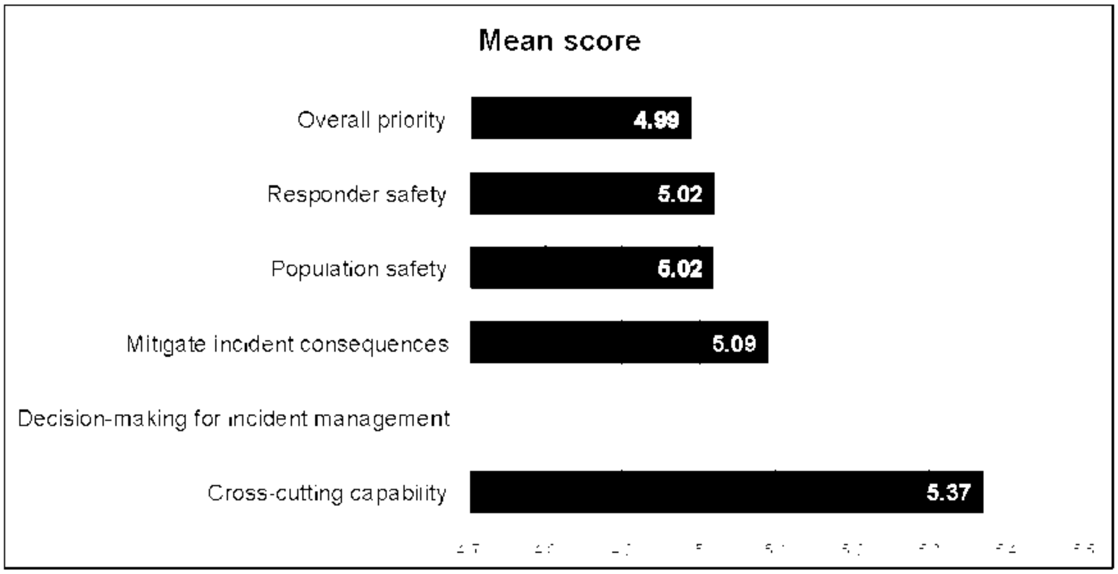


Figure 40. Mean Scores: ***ability to identify trends, patterns and important content from large volumes of information from multiple sources (including nontraditional sources) to support incident decision-making***

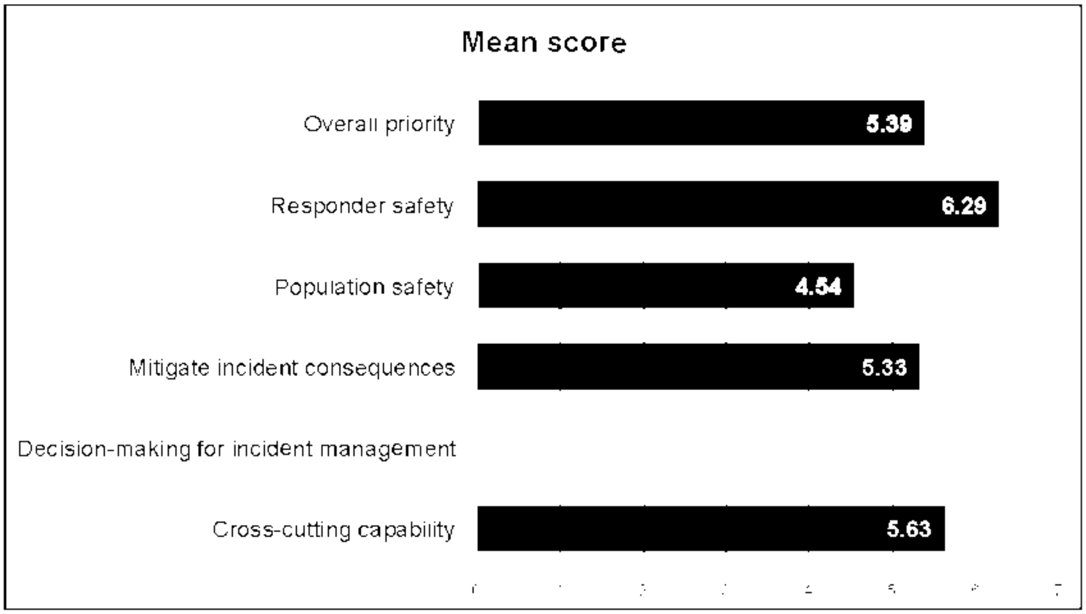


Figure 41. Mean Scores: ***protective clothing and equipment for all responders that protects against multiple hazards***

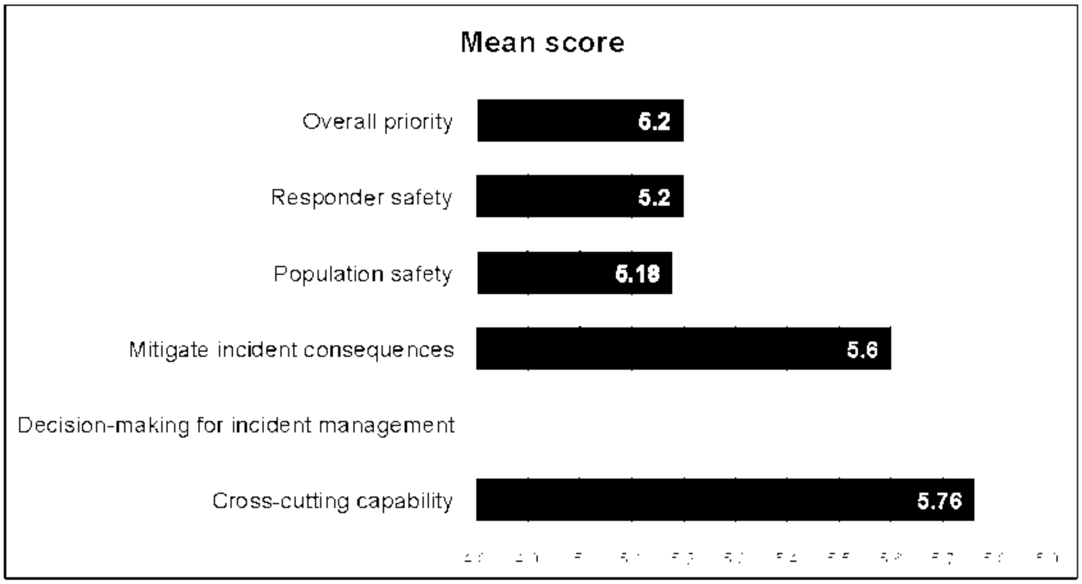


Figure 42. Mean Scores: ***ability to identify what resources are available to support a response (including resources not traditionally involved in response), what their capabilities are and where they are, in real time***

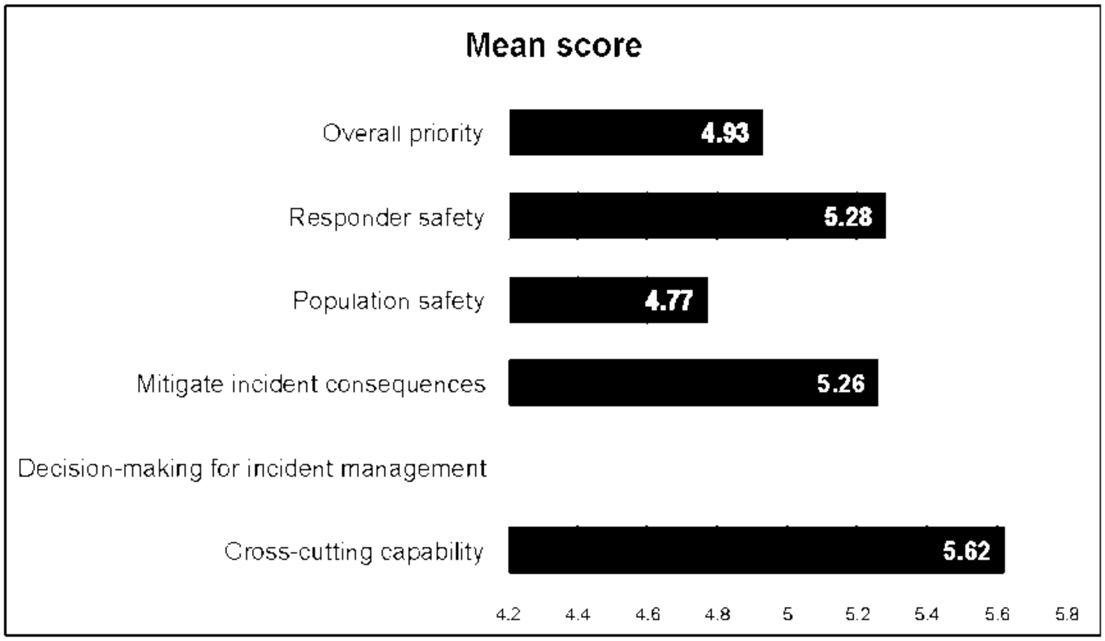


Figure 43. Mean Scores: ***ability to monitor the status of resources and their functionality in current conditions, in real time***

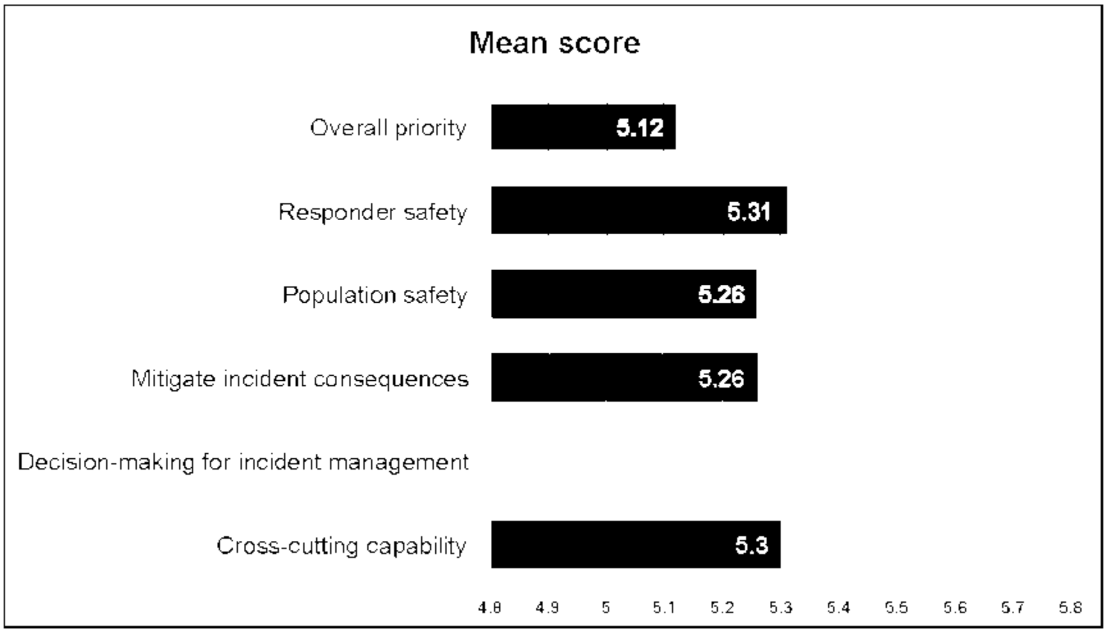


Figure 44. Mean Scores: ***ability to remotely scan an incident scene for signs of life and decomposition to identify and locate casualties and fatalities***

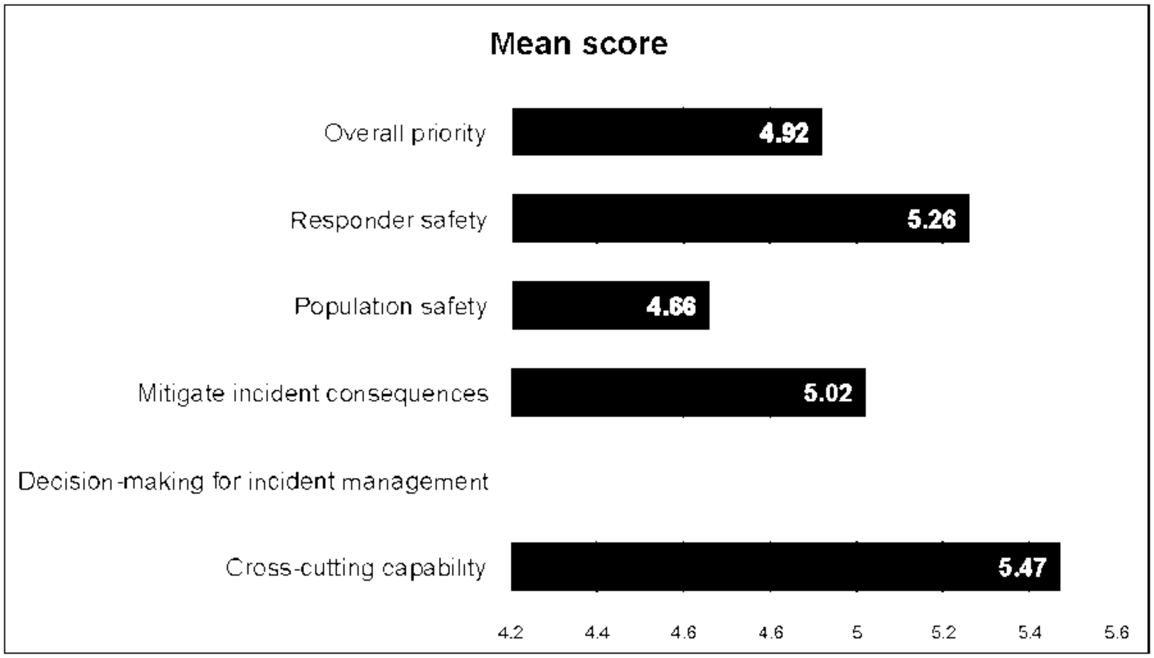


Figure 45. Mean Scores: ***readily accessible, high-fidelity simulation tools to support training and exercises in incident management and response***

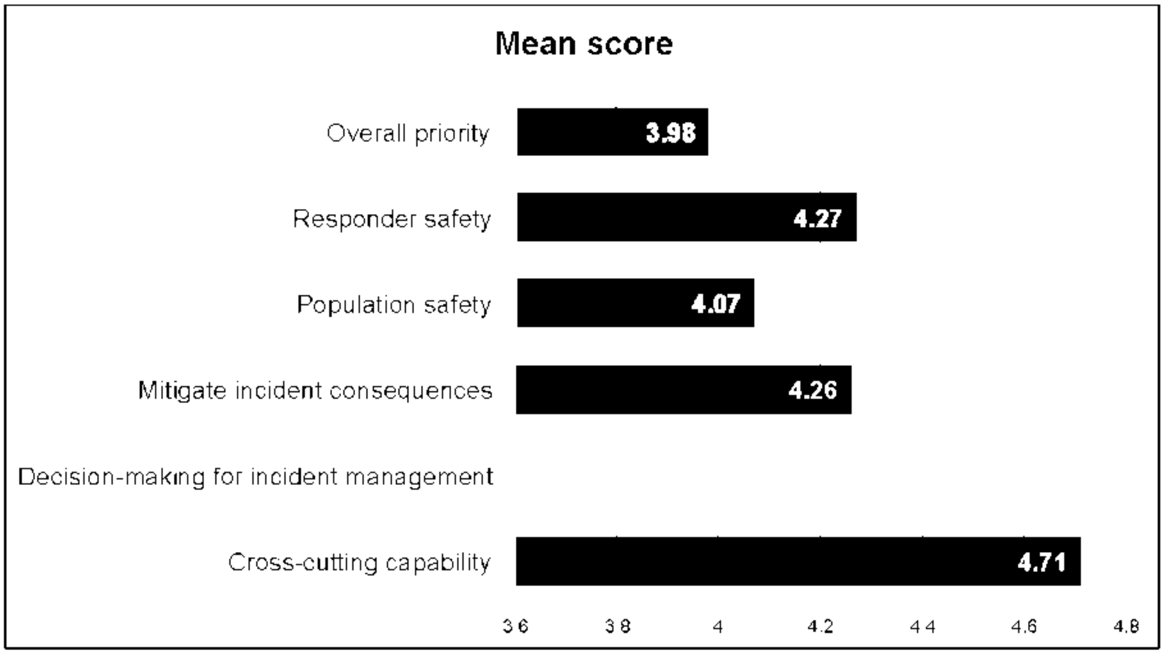


Figure 46. Mean Scores: ***ability to identify, assess and validate emergency response-related software applications***

Results of this prioritization process provide insight from responders on what the critical needs are for an effective response to a catastrophic incident. This insight should be used to help focus additional research and investment decisions for eventual technology development, transition and implementation. Particularly, the priorities shown in figure 30 for each discipline may be helpful for developers to understand who their primary customer may be for requirements generation and technology development. Other visualizations provided help decision-makers understand how the anticipated investments align with responder priorities.

APPENDIX D. PROJECT RESPONDER 4 PARTICIPANTS

Name	Organization
(b)(6)	Los Angeles City, CA, Police Department
	Miami-Dade County, FL, Emergency Management
	National Aeronautics and Space Administration
	Louisiana State University Health Sciences Center
	Washington, DC, Capitol Police (Ret)
	North Carolina State University
	San Francisco, CA, Fire Department
	National Institute of Standards and Technology
	Texas Task Force 1
	Applied Research Associates
	First Responder Network Authority
	Christine Wireless, Inc.
	Virtual Heroes
	Fairfax County, VA, Emergency Management Agency
	Milliken, CO, Police Department
	Florida Department of Highway Safety and Motor Vehicles
	University of Toledo, Public Health and Homeland Security
	Carnegie Mellon Software Engineering Institute
	California Department of Corrections and Rehabilitation
	Department of Homeland Security, Customs and Border Protection
	Idaho National Laboratory
	Idaho National Laboratory
	Intermedix
	General Dynamics
	Ohio State Department of Public Safety
	Worcester Polytechnic Institute
	Oolaga-Talala Emergency Medical Services
	Point White Partners
	Google
	Idaho National Laboratory

Name	Organization
(b)(6)	North Carolina State University
	Arizona State Police
	Worcester Polytechnic Institute
	Honolulu, HI, Emergency Medical Services
	Charlotte, NC, Fire Department
	Arlington, VA, Fire Department
	Seattle, WA, Fire Department
	Chicago Fire Department
	Central Islip Hauppauge Volunteer Ambulance
	Carnegie Mellon Software Engineering Institute
	Association of Public-Safety Communications Officials
	Alexandria, VA, Emergency Management Agency
	Ncoded Communications
	Pennsylvania 3rd Civil Support Team
	Boston, MA Fire Department
	Nugenis, LLC
	Department of Defense Office of the Secretary of Defense Domestic Preparedness Support Initiative
	Federal Emergency Management Agency/U.S. Fire Administration
	Massachusetts Department of Public Health
	Salem, NY, Volunteer Fire Department
	New York, NY, Fire Department
	Seattle, WA, Fire Department
	New Braunfels, TX, Emergency Management Agency
	National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory
	Muskogee County, OK, Emergency Medical Services
	Moore, OK, Fire Department
	First Responder Network Authority
	Applied Research Associates
	New York, NY, Fire Department
	Carnegie Mellon Silicon Valley
	Cal Maritime, California State University
	Arlington, VA, Fire Department

Name	Organization
(b)(6)	Resgrid
	Applied Communications Sciences
	San Diego, CA, Emergency Medical Services
	Applied Research Associates
	Association of Local Emergency Managers
	Robotic Research, LLC
	Oklahoma State University
	Department of Homeland Security, Science and Technology Directorate
	Comal County, TX, Emergency Management Agency
	National Association of Emergency Medical Technicians
	Jet Propulsion Laboratory (NASA)
	Charleston County, SC, Sheriff's Office
	Los Angeles Fire Department (Ret)
	American Medical Response
	Idaho National Laboratory
	New York State Police (Ret)
	NodeSource
	Virtual Alabama
	San Antonio Fire Department
	New York, NY, Police Department
	Defense Advanced Research Projects Agency
	Huntingdon County, PA, Emergency Management Agency
	U.S. Army Research Laboratory
	National Institute of Standards and Technology
	Department of Homeland Security, Office of Health Affairs
	Globe
	Plantation, FL, Fire Department
	ConEdison
	South Central Pennsylvania Regional Task Force
	State of Alabama Fire Marshal
	TRX Systems, Inc.
	Department of Homeland Security, Science and Technology Directorate

Name	Organization
(b)(6)	Federal Emergency Management Agency
	National Institute of Environmental Health Sciences
	Apple
	Applied Science Foundation for Homeland Security
	Littleton, CO, Fire Department
	Tualatin Valley Fire & Rescue
	Louisiana State University-Stephenson Disaster Management Institute
	Arlington County VA, Fire Department
	Homeland Defense and Americas' Security Affairs
	Metro Transit Police Department, Washington DC
	Salve Regina University
	National Highway Traffic Safety Administration
	Society for Simulation in Health Care
	New York, NY, Fire Department (Ret)
	Environmental Protection Agency
	National Institute of Standards and Technology
	International Personal Protection, Inc.
	National Sheriffs Association
	Virginia Department of Emergency Management
	Carnegie Mellon Software Engineering Institute
	Texas Department of State Health Services
	TRX Systems, Inc.
	Public Safety and Homeland Security, Commonwealth of VA
	North Carolina State University
	Carrollton, TX, Fire Rescue
	New York, NY, Fire Department (Ret)
	Idaho National Laboratory
	U.S. Forest Service National Interagency Fire Center
	Delaware Emergency Management Agency
	San Diego, CA, Fire Rescue
	Seattle, WA, Fire Department
	Department of Homeland Security, Immigration and Customs Enforcement, Office of the Chief Information Officer

Name	Organization
(b)(6)	Idaho National Laboratory
	Santa Clara County, CA, Sheriff
	North Dakota Department of Public Health
	Prescott, AZ, Fire Department

APPENDIX E. ACRONYMS

Acronym	Definition
AIS	Automatic Identification Systems
ANS	Adaptable Navigation Systems
AI	Artificial Intelligence
API	Application Programming Interface
ARGUS-IR	Autonomous Real-Time Ground Ubiquitous Surveillance - Infrared
ART	Adaptive RF Technology
AWARE	Advanced Wide FOV Architectures for Image Reconstruction and Exploitation
B2B	Business-to-Business
C3	Command, Control, and Coordination
CAD	Computer-Aided Dispatch
CAMEO	Computer-Aided Management of Emergency Operations
CATS	Consequence Assessment Tool Set
CCTV	Closed-Circuit Television
CIAB	Cell in a Box
CIKR	Critical Infrastructure and Key Resources
CIMS	Civil Support Team Information Management System
CMUVT	Compact Mid-Ultraviolet Technology
COLTS	Cell on Light Trucks
COP	Common Operating Picture
COTS	Commercial Off-the-Shelf
COWS	Cellular on Wheels
CSFV	Crowd Sourced Formal Verification
CST	Civil Support Teams
CTTSO	Office of Combating Terrorism Technical Support Office
D2P	Detect-to-Protect
DARPA	Defense Advanced Research Projects Agency
DBM	Distributed Battle Management
DHS	Department of Homeland Security
DM2	DoD Meta Model
DOD	Department of Defense
DoDAF	DoD Architecture Framework

Acronym	Definition
DTRA	Defense Threat Reduction Agency
EA	Edge Analytics
ECG	Electrocardiography
ECWCS	Extended Climate Warfighter Clothing System
EDGE	Enhanced Dynamic Geo-Social Environment
EGVs	Unmanned Ground Vehicles
EMP	Electromagnetic Pulse
EMS	Emergency Medical Services
EMT	Emergency Medical Technician
EOD	Explosive Ordnance Disposal
EPIRB	Emergency Position Indicating Radio Beacons
ERG	Emergency Response Guidebook
EXIF	Exchangeable Image File Format
FAA	Federal Aviation Administration
FBCB2/BFT	U.S. Army's Force XXI Battle Command Brigade-and-Below/Blue Force Tracking
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FINDER	Finding Individuals for Disaster and Emergency Response
FirstNet	First Responder Network Authority
FLIR	Forward-Looking Infrared
FREE	Flame Resistant Environmental Ensemble
FOV	Field of view
FRG	Support to the Homeland Security Enterprise and First Responders Group
FRRG	First Responders Resource Group
GLANSER	Geospatial Location Accountability and Navigation System for Emergency Responders
GPR	Ground-Penetrating Radar
GPS	Global Positioning System
GUI	Graphical User Interface
HAZMAT	Hazardous Materials
HITECH	Health Information Technology for Economic and Clinical Health

Acronym	Definition
HMI	Human-Machine Interface
HPAC	Hazard Prediction and Assessment Capability
HSARPA	Homeland Security Advanced Projects Agency
HSSAI	Homeland Security Studies and Analysis Institute
HUD	Heads Up Display
IAB	InterAgency Board
IBC	International Building Code
ICS	Incident Command System
IEC	International Electrotechnical Commission
ILMS	Integrated Logistics Management System
IMAAC	Interagency Modeling and Atmospheric Assessment Center
IMU	Inertial Measurement Units
ISO	International Organization for Standardization
IT	Information Technology
JPL	NASA Jet Propulsion Laboratory
JSON	Javascript Object Notation
KML	Keyhole Markup Language
KMZ	Keyhole Markup Language Zipped
LDM	Logical Data Model
LELs	Lower Explosive Limits
LIDAR	Light Detection and Ranging
LSCMS	Logistics Supply Chain Management System
LTE	Long Term Evolution
MDC	Mobile Data Computers
MERC	Medical Emergency Response Center
Micro-PNT	Micro-Technology for Positioning, Navigation and Timing
MIPT	Memorial Institute for the Prevention of Terrorism
MRSA	Methicillin-resistant Staphylococcus Aureus
NESC	National Exercise and Simulation Center
NFPA	National Fire Protection Association
NGA	National Geospatial Agency
NHC	National Hurricane Center
NIEM	National Information Exchange Model
NIMS	National Incident Management System

Acronym	Definition
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NPC	Non-Player Characters
NPD	National Preparedness Directorate
NSRDC	U.S. Army Natick Soldier Research and Development Center
NTRO	National Terrorism Response Objectives
NwHIN	Nationwide Health Information Network
ORD	Operational Requirements Document
OSHA	Occupational Health and Safety Administration
PAGER	Prompt Assessment of Global Earthquakes for Response
PASS	Personal Alert Safety System
PES	Physical Exchange Specification
PHASER	Physiological Health Assessment System for Emergency Responders
PLB	Personal Locator Beacons
PPE	Personal Protective Equipment
PR3	Project Responder 3
PR4	Project Responder 4
RAN	Radio Access Network
RAPS	Robotic Aircraft for Public Safety
REMM	Radiation Emergency Medical Management
RF	Radio Frequency
RFID	Radio Frequency Identification
RKB	Responder Knowledge Base
ROSS	Resource Ordering and Status System
ROV	Remotely Operated Vehicles
RTO	Response Technology Objectives
S&T	Science and Technology Directorate
SAFER	Safer Warfighter Communications
SCBA	Self-Contained Breathing Apparatus
SDK	Software Development Kit
SELC	Software Engineering Lifecycle
SLAM	Uses Simultaneous Location and Mapping
SMS	Short Message Service
SOO	Statement of Objectives

Acronym	Definition
STA	Special Temporary Authorization
STTC	U.S. Army's Simulation and Training Technology Center
SUAS	Small Unmanned Aircraft Systems
SUMMIT	Standard Unified Modeling, Mapping, and Integration Toolkit
SWAT	Special Weapons and Tactics
TRRN	Texas Regional Resource Network
TSWG	Technical Support Working Group
TTP	Tactics, Techniques, and Procedures
UAS	Unmanned Aerial Systems
UHF	Ultra High Frequency
ULTRA-Vis	Urban Leader Tactical Response, Awareness and Visualization
USGS	United States Geological Survey
UV	Ultraviolet
VOCs	Volatile Organic Compounds
VoIP	Voice Over Internet Protocol
VoLTE	Voice Over Long Term Evolution
WASP	Wearable Advanced Sensor Platform
XML	Extensible Markup Language

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

August 25, 2015

MEMORANDUM FOR COMPONENT HEADS

FROM: Jeh Charles Johnson
Secretary

SUBJECT: **Establishment of Integrated Product Teams**

As the Department continues to improve acquisition and research and development (R&D) processes across DHS to deliver technologies and close identified capability gaps, I am directing the re-establishment of the Science and Technology Directorate's (S&T) Integrated Product Teams (IPT). The IPTs will be aligned to the DHS mission areas and will incorporate an S&T-led technology assessment for all major acquisitions in the Department. These efforts will broaden and deepen the Unity of Effort Initiative.

IPTs are cross-DHS entities that are tasked to identify DHS technological capability gaps and coordinate R&D to close those gaps across the mission areas of the Department. The overall IPT effort will be led by S&T, but the individual IPTs will be led by senior representatives from the operational Components with representation from Joint Requirements Council Portfolio Teams and support from S&T. The IPT topic areas will initially address: Aviation Security (DHS Core Mission 1), Biological Threat (Mission 1), Counterterrorism (Mission 1), Border Security (Mission 2), and Cyber Security (Mission 4).

Going forward, IPTs will be the central mechanism by which the Department identifies and coordinates its R&D efforts to DHS priority missions. The IPT process will ensure that the Department is investing in non-duplicative technologies that directly address Component capability gaps as efficiently and effectively as possible.

Initially the IPTs will accomplish the following:

1. Identify and prioritize DHS capability gaps and corresponding technology solutions to close those gaps.
2. Identify R&D work being performed across DHS, both in traditional R&D funding lines and that occurring within Component acquisition programs.
3. Ensure technology being acquired will meet DHS and Component mission needs.
4. Identify and de-conflict duplicative R&D efforts.
5. Develop and report metrics for the transition of technological solutions to close capability gaps.

~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, copying, or further distribution of this information to unauthorized individuals (including unauthorized members of the President-elect Transition Team) is strictly prohibited. Unauthorized disclosure or release of this information may result in loss of access to information, and civil and/or criminal fines and penalties.~~

Output of the IPTs will be briefed to the JRC. These activities will culminate in two products: 1) the Report of Coordinated DHS R&D, which will capture all of the Department's ongoing R&D activities, and 2) the S&T High Priority Technology Solutions document, which will capture the priority solutions to capability gaps to guide S&T's R&D work to meet the needs of the operational Components.

S&T will conduct a system engineering review and technology assessment of the technical solutions in DHS major acquisition programs and provide a report to the Chief Acquisition Officer and Joint Requirements Council prior to the decision to enter the "Obtain" phase of the Acquisition Life Cycle. This will ensure that S&T is involved early in the acquisition process to assess the technical maturity of the technologies that DHS major acquisitions intend to acquire.

I have instructed Under Secretary Brothers to meet with each of you to discuss the details of the IPT process and gather your feedback on how to make this a successful initiative. I ask that you give him your full support in this process. In the coming months, there will be an update to the appropriate Directives and Instructions formally codifying the IPT and Technology Assessment process.

Science and Technology Directorate Brief

Agency Review Team

December 14, 2016

Deputy Under Secretary Dr. Robert Griffin

High Level Description

Homeland Security

Science and Technology

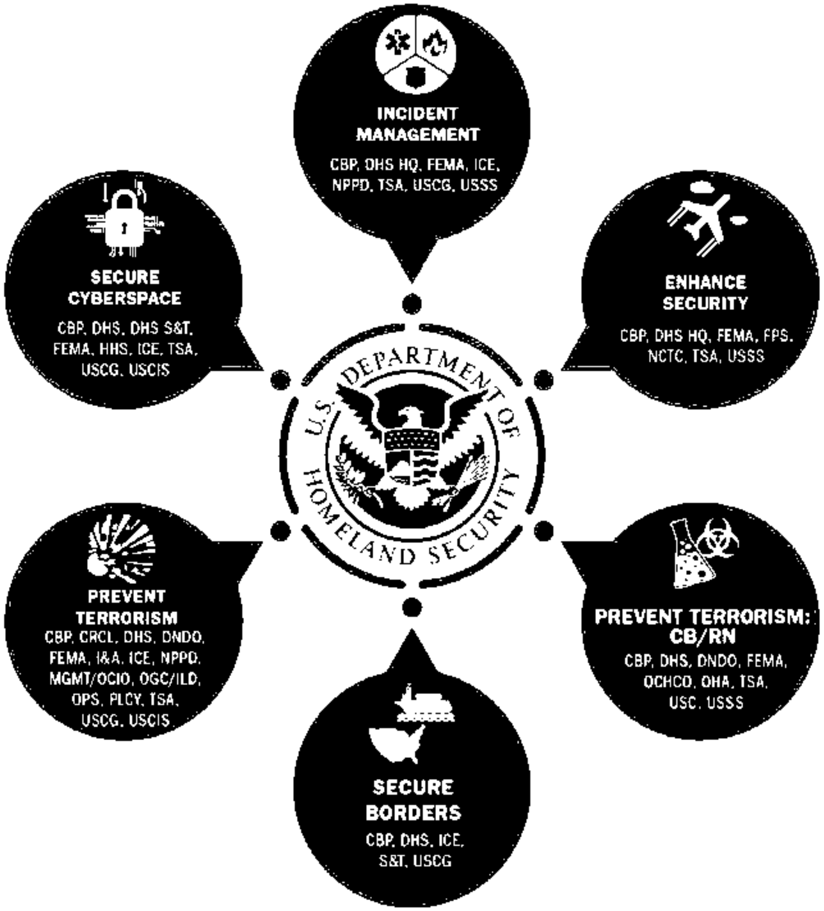
- Science and Technology Advisor to the Secretary, DHS Components, and First Responders.
- Identifies High-Priority Technological Capability Gaps to Meet Homeland Security Threats.
- Leads Engagement of Government, Industry, and Innovation Partners to Develop and Leverage Needed Technologies.
- Transitions Technology and Knowledge to Meet Critical Homeland Security Needs by Providing Cross-Cutting Technology, Subject Matter Expertise, and Knowledge Products.
- Acts as the Test and Evaluation Agent for the Secretary on Major Acquisition Programs.

S&T Impact on DHS Operations

- **Mitigating High-Profile National Threats** – Brought expertise and new technology solutions to major operational events. For example: Unmanned Aerial System Modeling and Simulation Capabilities with the USSS for the 2016 Political Conventions.
- **Securing Airspace and Air Travel** – Worked with components to categorize explosives, enhance innovation lanes in airports, improve recruitment, retention and training at the Transportation Security Administration. For example: Assisted in the development, deployment, and use of Biometric Entry with CBP at U.S. Air Ports of Entry.
- **Strengthening Immigration and Customs Processes** – Worked across DHS to enable improved vetting of K-1 visa and refugee applications. For example: Social media analysis with USCIS on applications from Syria and Iraq.
- **Securing Borders** – Worked directly with CBP field offices to fill operational gaps at the border. For example: Developed and deployed improved tunnel detection, communication interoperability, and low-cost ground sensors.
- **Making First Responders Safer and More Effective / Responding to Natural Disasters** – Enhanced first responder capabilities and gear. For example: Developed and deployed Finding Individuals for Emergency Response "FINDER" technology which identifies human heartbeat in rubble piles.
- **Creating Cyber Solutions** – Worked with cyber security industry to provide tools to prevent cyber attacks and crime. For example: Developed a tool for law enforcement to extract evidence from vehicle infotainment and navigation systems.
- **Combatting Human Trafficking** – Developed and deployed a non-cooperative biometrics capability to protect children. For example: DHS Homeland Security Investigations used the imagery to identify and rescue 350 children from sex abuse and human traffickers.

Linkage to DHS Priorities /Missions

- DHS-Wide R&D Plan
- First Responder R&D Plan
- Immediate Response to Emerging Threats
- Directed R&D
  - President
  - Congress
  - National Security Council
  - Secretary



INCIDENT MANAGEMENT
CBP, DHS HQ, FEMA, ICE, NPPD, TSA, USCG, USSS

ENHANCE SECURITY
CBP, DHS HQ, FEMA, FPS, NCTC, TSA, USSS

PREVENT TERRORISM: CB/RN
CBP, DHS, DNDO, FEMA, OCHCO, OHA, TSA, USC, USSS

SECURE BORDERS
CBP, DHS, ICE, S&T, USCG

PREVENT TERRORISM
CBP, CRCL, DHS, DNDO, FEMA, I&A, ICE, NPPD, MGMT/OCIO, OGC/ILD, OPS, PLCY, TSA, USCG, USCIS

SECURE CYBERSPACE
CBP, DHS, DHS S&T, FEMA, HHS, ICE, TSA, USCG, USCIS

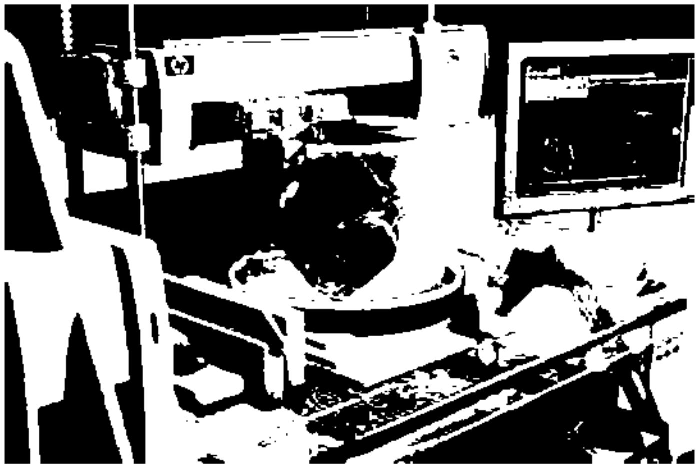
DHS Integrated Product Teams

Other Areas of Focus

- Asserting the Critical Role of Technology in Today's Operations and Shaping Future Operations.
- Increasing Efficiency and Effectiveness through Technology Foraging, Leveraging Public/Private Partnerships, and Invigorating Industrial Base.
- Ensuring Technology Gets into the Hands of Operators by Linking R&D into Acquisitions and Grants.
- Ensuring Timely Transition to Operations by Providing Robust Cradle-to-Grave Technical and Cyber Resources.
- Increasing S&T's Role in the Interagency to Encourage Collaboration/Partnership/Efficient Development, particularly DOD, DOJ, DOE, DOT.
- Changing the Nature of S&T's Workforce.
- Additional S&T Assets: Laboratories; Federally-Funded Research and Development Centers; University Centers of Excellence; Non-Traditional and Small Businesses; and International R&D Partnerships.

Leadership Perspective: Concerns/Challenges/Opportunities

- Pace of Technology Development Dramatically Changing Operational Risk and Threat.
- Expanding Scope, and Potential Impact and Vulnerabilities of Cyber Threat.
- Changing Needs of Forensics to Meet Technology Adaptations and Malignant Innovation.
- Increasing Quantity of Data and Operational Opportunities and Limitations of Big Data Analytics.
- Changing Nature of Chemical & Biological Threats.
- Inconsistent R&D Budget Levels.



Closing Takeaway

- S&T's R&D is focused on improving operations today and tomorrow, not just 10 years from now.
- S&T has a talented workforce - dedicated group of scientists, engineers and program managers solving complex problems for the operators in the field.
- S&T has a rigorous process to identify technological capability gaps and select proposed solutions to address DHS components' high-priority requirements.
- S&T is expanding tools, processes, and partnerships to accelerate operational adoption and use of solutions.
- No matter the threat or challenge, S&T rapidly develops and delivers knowledge, analyses, and innovative system solutions to advance the DHS mission.

Background

S&T Stats At-A-Glance

85
Current R&D Programs

27
Non-R&D Programs & Services

5
DHS Labs

10
University based Centers of Excellence

39
DHS Issued & Pending Patients as of FY16

881
SBIR[1] Awards as of FY16

486
Federal Employees

2
DHS Federally Funded R&D Centers (FFRDCs)

13
International Bilateral Agreements

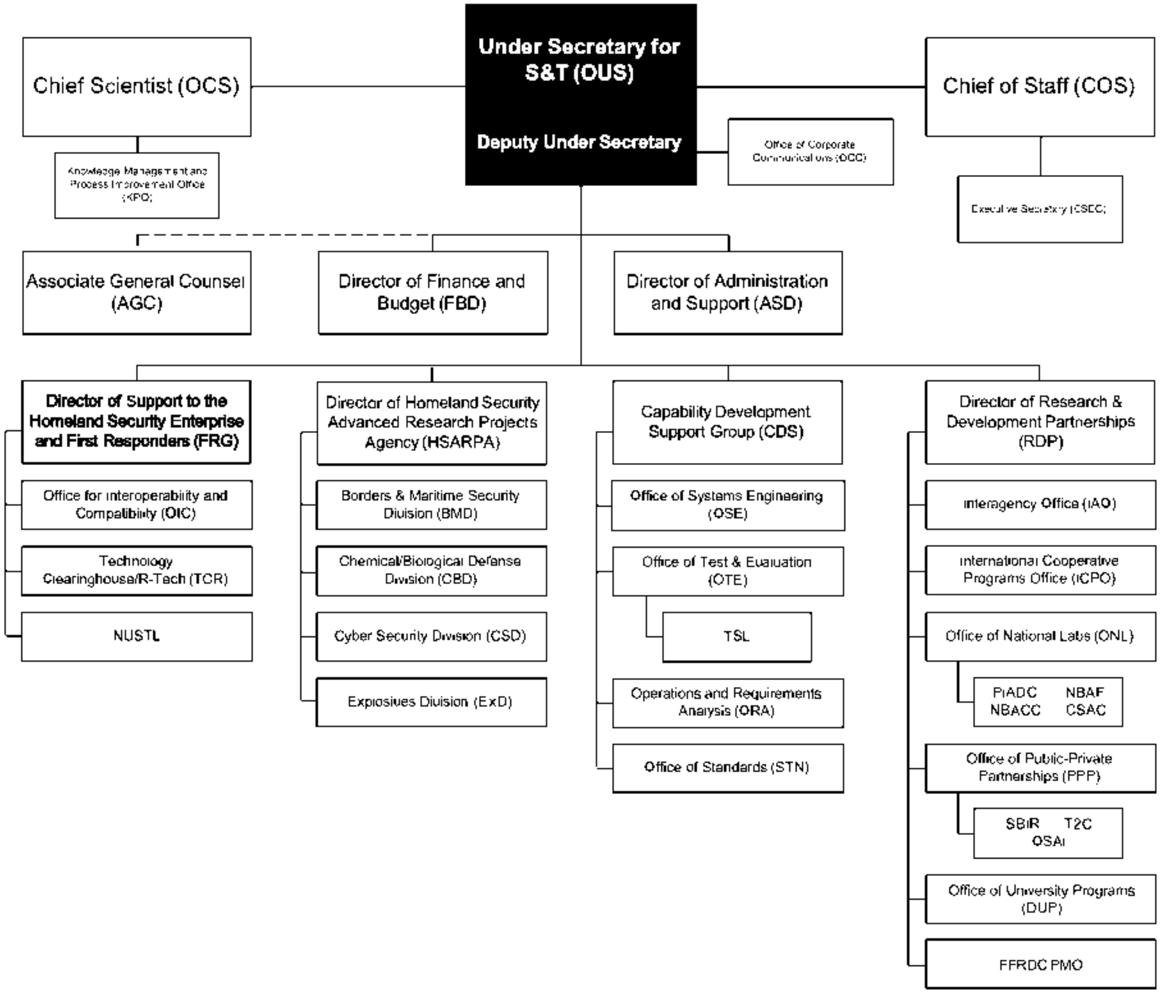
869
SAFETY[2] Act Total Approvals

+7%
Improvement in FEVS (largest in DHS HQ)

100%
Responsive to Secretary Requests

[1] Small Business Innovation Research (SBIR); [2] Support Anti-Terrorism by Fostering Effective Technologies (SAFETY)

Science and Technology Directorate



Under Secretary for S&T (OUS)

Deputy Under Secretary

Chief Scientist (OCS)

Knowledge Management and Process Improvement Office (KPO)

Office of Corporate Communications (OCC)

Chief of Staff (COS)

Executive Secretary (ESEC)

Associate General Counsel (AGC)

Director of Finance and Budget (FBD)

Director of Administration and Support (ASD)

Director of Support to the Homeland Security Enterprise and First Responders (FRG)

- Office for Interoperability and Compatibility (OIC)
- Technology Clearinghouse/R-Tech (TCR)
- NUSTL

Director of Homeland Security Advanced Research Projects Agency (HSARPA)

- Borders & Maritime Security Division (BMD)
- Chemical/Biological Defense Division (CBD)
- Cyber Security Division (CSD)
- Explosives Division (ExD)

Capability Development Support Group (CDS)

- Office of Systems Engineering (OSE)
- Office of Test & Evaluation (OTE)
  - TSL
- Operations and Requirements Analysis (ORA)
- Office of Standards (STN)

Director of Research & Development Partnerships (RDP)

- Interagency Office (IAO)
- International Cooperative Programs Office (ICPO)
- Office of National Labs (ONL)
  - PIADC NBAF NBACC CSAC
- Office of Public-Private Partnerships (PPP)
  - SBIR T2C OSAI
- Office of University Programs (OUP)
- FFRDC PMO