PARTNERSHIP GUIDE

Research Priorities and Collaboration Opportunities

Science and Technology

TABLE OF CONTENTS

OVERVIEW

At the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), we know there is great power in partnerships. In our work to deliver effective and innovative scientific and technological insights, methods, standards, and solutions for homeland security, we leverage a broad network of partners to help fulfill mission requirements.

As the research, development, test, and evaluation (RDT&E) arm for DHS, it is our job to ensure the Department has the solutions of today and tomorrow to secure our nation in the face of evolving threats. But we can't do it alone. S&T relies on our partners to identify and develop innovative technologies for homeland security. S&T provides unique business opportunities, contract mechanisms, and supports development of innovative technologies for homeland security.

WE WANT TO GROW OUR NETWORK OF PARTNERS TO DEVELOP HOMELAND SECURITY SOLUTIONS

OUR CUSTOMERS

Countering Weapons of Mass Destruction Office (CWMD)

Customs and Border Protection (CBP)

Cybersecurity and Infrastructure Security Agency (CISA)

Federal Emergency Management Agency (FEMA)

Federal Law Enforcement Training Center (FLETC)

Transportation Security Administration (TSA)

U.S. Citizenship and Immigration Services (USCIS)

U.S. Coast Guard (USCG)

U.S. Immigration and Customs Enforcement (ICE)

U.S. Secret Service (USSS)

DHS Headquarters Elements

State, Local, Tribal, Territorial First Responders

Other Federal Agency Partners

Homeland Security Enterprise (HSE)

DHS MISSION AREAS

Counter Terrorism and Homeland Threats

Secure U.S. Borders

Secure Cyberspace and Critical Infrastructure

Preserve and Uphold the Nation's Prosperity and Economic Security

Strengthen Preparedness and Resilience

Champion the DHS Workforce and Strengthen the Department

S&T'S RDT&E FOCUSES ON THE FOLLOWING TYPES OF SOLUTIONS

NEAR-TERM COMPONENT

Includes projects/activities that focus on gaps or needs that have been identified by DHS components.

FOUNDATIONAL SCIENCE

Enduring research that results in better and more actionable data sets, knowledge products, standards, and peer-reviewed publications to support scientific endeavors.

FUTURE NEEDS AND EMERGING THREATS

Exploring emerging science and technology areas and their potential threat or application to future DHS missions.

INNOVATION ECOSYSTEM

S&T's innovation ecosystem is a network of government and private sector entities across the globe that work together to address a range of current and emerging threats—from aviation security to chemical and biological detection to critical infrastructure, resilience, climate and natural disasters, cybersecurity, and beyond. By leveraging relationships with our network of partners, we remain an effective catalyst for improving the strength and resilience of our nation.

Learn about our Partnership Pathways on page 12 and discover how you can tap into S&T's innovation ecosystem.

Sign up for S&T's Partnership Connections and Program Mailing Lists to receive news and updates on a range of S&T's solicitations, program information, and events.

https://go.dhs.gov/JUA

S&T's Industry Liaison is your primary entry point into S&T. Email us or check out our website.

SandT.Innovation@hq.dhs.gov
www.dhs.gov/science-and-technology/work-with-st

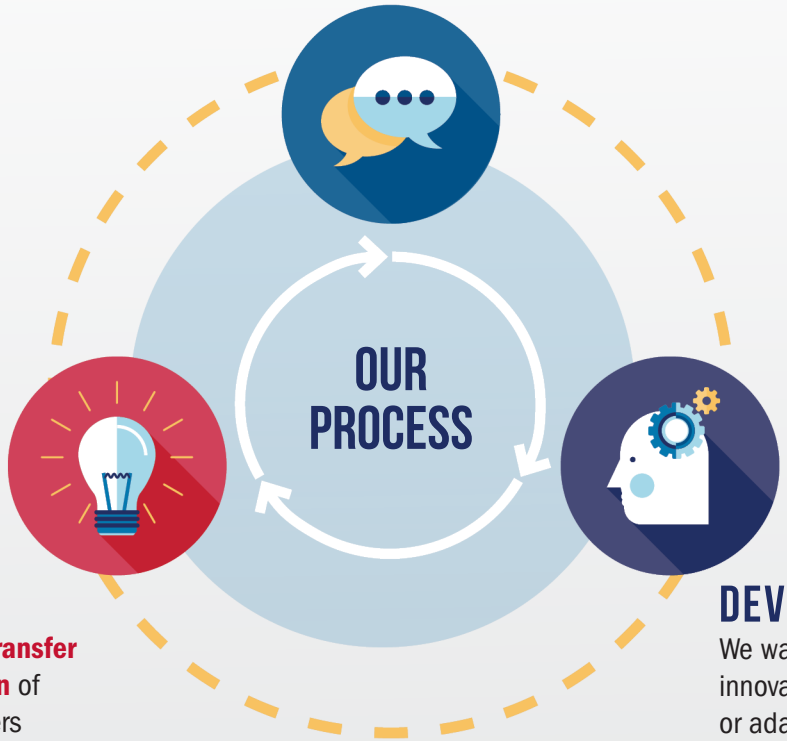
You can also tell us about your capabilities and what you have to offer by filling out our Industry Outreach Form.

www.dhs.gov/publication/st-dhs-industry-outreach-form

WE NEED YOUR HELP TO DISCOVER SCIENTIFIC ADVANCEMENTS AND TECHNOLOGICAL INNOVATIONS THAT SOLVE HOMELAND SECURITY CHALLENGES

ENGAGE

We want to **connect** with innovators and **discover** unique ideas, prototypes, and technologies that can address homeland security challenges.



DELIVER

We want support the **transfer** and **commercialization** of capabilities to end-users and the homeland security marketplace.

DEVELOP

We want to **partner** with innovators to develop new, or adapt existing, solutions to meet the Department's numerous operational needs.

OUR PARTNERS AND CAPABILITIES

Through parnerships with a variety of entities, S&T provides pathways to external RDT&E investments and non-traditional performers, sponsors cutting-edge technology and capability development, and delivers high-impact solutions for S&T customers.

ACADEMIA

S&T streamlines access to the expertise of the nation's colleges and universities to address pressing homeland security needs. This includes programs that bring together university-led, multi-disciplinary consortia of scientists, mathematicians, and engineers from across the nation along with public and private sector partners. These researchers investigate important questions relevant to homeland security and develop new technologies and methodologies to solve complex homeland security problems.

For more information, visit **www.dhs.gov/science-and-technology/office-university-programs** or contact **universityprograms@hq.dhs.gov**.

FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS (FFRDCS)

FFRDCs act as a vehicle for special research and development contracting within the federal government that perform high-quality research and provide advice that is authoritative, objective, and free from conflicts of interest caused by competition. S&T's FFRDCs provide DHS with independent and objective advice and quick response on critical issues throughout the HSE.

For more on S&T's work with FFRDCs, visit **www.dhs.gov/science-and-technology/ffrdcs** or contact **ST.FFRDC@hq.dhs.gov**.

INDUSTRY

S&T engages and cultivates relationships with industry stakeholders to identify, develop and deliver cutting-edge technologies for the homeland security mission and transfer federally funded technology into the marketplace. S&T provides unique business opportunities that incentivize industry to develop and commercialize innovative and mission-relevant technologies.

For more information, visit **www.dhs.gov/science-and-technology/work-with-st** or contact **SandT.Innovation@hq.dhs.gov**.

INTERNATIONAL

S&T works with and engages foreign governments, international institutions, and global networks as well as industry to accelerate capability development and transition, enhance affordability, and take advantage of emerging ideas and solutions. International partnerships can help further the DHS mission, facilitate bilateral and multilateral technical fora, support policy and operational global engagement on science and technology matters and plans, and help implement the Under Secretary's unique authorities for international cooperative activities. For more information, visit **www.dhs.gov/science-and-technology/st-icpo** or contact **SandT.InternationalPrograms@HQ.DHS.GOV**.

NATIONAL LABORATORIES

S&T's coordinated network of laboratories provides a centralized laboratory-based RDT&E function for the entire Department. This network includes S&Ts own national laboratory capabilities and sites, which align with core RDT&E needs of DHS, and features streamlined access to Department of Energy National Laboratories as well as facilitated access to other government labs throughout the interagency. These labs leverage partnerships with industry to help fulfill homeland security mission needs.

For more information, visit **www.dhs.gov/science-and-technology/office-national-laboratories** or contact **ONLUtilization@hq.dhs.gov**.

We are always looking to expand our network and engage new innovators! There are so many ways to connect, and we are looking forward to hearing from you.

SUMMARY OF RDT&E PRIORITIES

Protecting our nation requires timely response to rapidly evolving dangers while protecting against longer-term threats to the homeland. To fully understand the needs of our operational components, we identify priorities that require solutions in key mission-focused areas.

The priority needs in these areas drive S&T's RDT&E investments and we're looking for organizations ready to partner with us.

www.dhs.gov/publication/st-dhs-industry-outreach-form

For the details about our RDT&E priorities see the directory starting on page 22.

BORDER SECURITY

- Air, Land and Port of Entry (POE) Security
- Biometrics and Identity Management
- Counter Unmanned Aircraft Systems
- Forensic and Criminal Investigations
- Immigration Services
- Maritime Safety and Security

CHEMICAL, BIOLOGICAL, AND EXPLOSIVE (CBE) DEFENSE

- Chem-Bio Detection
- Detection Canine Services
- Opioid/Fentanyl Detection

COUNTER TERRORISM

- Emerging Risks and Technologies
- Explosives Threat Assessment
- Probabilistic Analysis of National Threats, Hazards and Risks (PANTHR)

CYBERSECURITY / INFORMATION ANALYSIS

- Cybersecurity

FIRST RESPONDER CAPABILITIES

- Cargo/Baggage /People Screening
- Community and Infrastructure Resilience
- Countering Violent Extremism
- First Responder Capability
- Physical Security

PARTNERSHIP PATHWAYS

S&T is continually looking for new partners to help us develop and deliver the best technological innovations to the DHS workforce and safeguard our nation. We have unique tools for working with many kinds of innovators and we are looking to partner with you!

Learn about the ways you can ENGAGE with us, DEVELOP innovative technologies, and DELIVER solutions to homeland security end users.

The SAFETY Act Program incentivizes development and widespread deployment of effective anti-terrorism technologies by providing risk management and litigation protections to ensure that the threat of liability does not deter potential manufacturers or sellers from developing and commercializing innovations that could save lives. These evolving technologies may include a single product or combination of products, equipment, software, or services. The program engages with the public and private sectors to increase awareness of SAFETY Act protections, encourages best practices, promotes participation and collaboration, and builds partnerships with the developers of new anti-terrorism technologies for the protection of critical infrastructure, national security, and public safety.

For more information, visit SAFETYAct.gov.

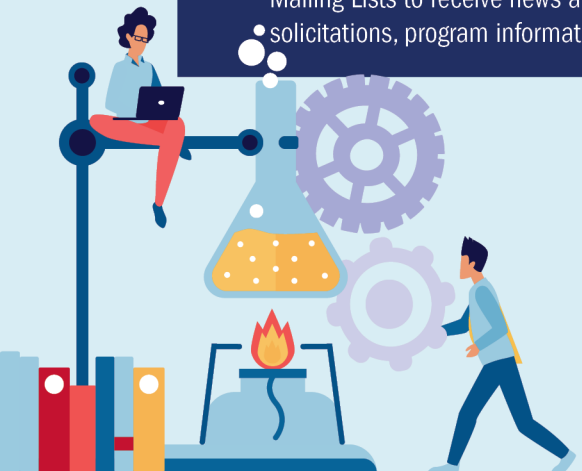
If you or your organization would like to tell us about your technology and receive news and updates from S&T about our opportunities, please fill out the DHS Industry Outreach Form at www.dhs.gov/publication/st-dhs-industry-outreach-form and submit back to SandT.Innovation@hq.dhs.gov.

ENGAGE

S&T's Industry Liaison is your primary entry point into S&T! DHS maintains a network of Industry Liaisons that foster strategic relationships with vendors and other stakeholders that seek to do business with the Department. **S&T's Industry Liaison** is a dedicated point of contact for private sector organizations to learn about S&T's mission and R&D needs. If you want to provide capability information, understand our requirements and opportunities, or get your questions answered, reach out to our Industry Liaison today at **SandT.Innovation@hq.dhs.gov**.

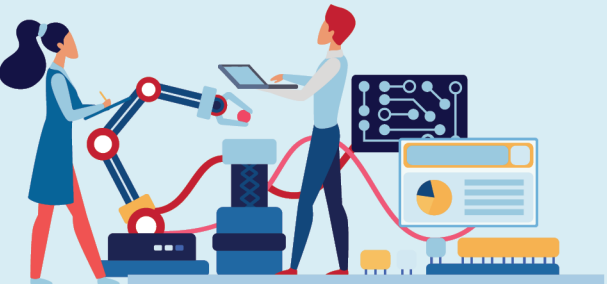
Not industry? We still want to hear from you regardless of your organization type. Our Industry Liaison can connect you to the right S&T point of contact.

Sign up for S&T's Partnership Connections and Program Mailing Lists to receive news and updates on a range of S&T's solicitations, program information, and events.



DEVELOP

Private sector innovation is a key to success for DHS S&T to develop new technologies to support homeland security R&D needs. S&T's **Innovation Funding Programs and Tools** are unique tools for working with many kinds of entities. Whether you are a small or large business, academia, or startup, we want you to help us innovate and advance homeland security solutions. Check out the table for eligibility requirements and read more on our programs to learn how you can innovate with S&T.



Binational Industrial Research and Development (BIRD) Program	Provides grants to U.S. and Israeli entities partnering to develop advanced technologies of mutual interest for homeland security (BIRD Homeland Security Program) and Cybersecurity (BIRD Cyber) missions www.dhs.gov/science-and-technology/bird-hls
In-Q-Tel Engagement	A resource for DHS and federal partners to find innovative and cutting-edge, venture-backed commercial technology. www.dhs.gov/science-and-technology/iqt
Long Range Broad Agency Announcement (LRBAA)	A standing invitation for members of the scientific and technical communities to propose novel solutions for RDT&E projects in support of our nation's security. www.dhs.gov/science-and-technology/st-lrbaa
Prize Competitions	Crowdsources innovation to harness the creativity of the American public to spur groundbreaking solutions to critical homeland security challenges. www.dhs.gov/science-and-technology/prize-competitions
Silicon Valley Innovation Program (SVIP)	Works with startups from around the world to develop and adapt innovative technology for operational missions. www.dhs.gov/science-and-technology/svip
Small Business Innovation Research (SBIR) Program	Works with U.S. small businesses to provide quality research and to develop new processes, products, and technologies in support of U.S. government missions. www.dhs.gov/science-and-technology/sbir
Targeted Broad Agency Announcement (BAA)	Time-sensitive topic solicitations that execute defined research and development to deliver practical solutions to homeland security priority needs oip.dhs.gov/baa/public

Please visit program websites for more specifics about eligibility requirements.

FIND YOUR INNOVATOR TYPE

- Medium to Large Businesses
- Small Businesses
- Entrepreneurs & Startups
- National Labs, Recognized R&D Organizations
- Academia
- Private Citizens
- International

For more information, visit
www.dhs.gov/science-and-technology/office-public-private-partnerships

DELIVER

S&T's **Technology Transfer and Commercialization** (T2C) is the central point to manage technology transfer activities throughout DHS and the DHS laboratory network. Technologies developed and evaluated within the Department can have tremendous potential for commercial applications throughout the nation, enhance the competitiveness of individual small businesses, and expand areas of exploration and cooperation for all non-federal partners.

Read more at **www.dhs.gov/science-and-technology/technology-transfer-program** or contact us at **T2C@hq.dhs.gov** to learn about DHS technologies that are available for licensing and the T2C mechanisms.

Intellectual Property and General Licensing	T2C supports the protection of DHS-funded intellectual property (IP) through patents, trademarks, or copyrights; licenses DHS-owned IP, and disburses license royalties Department of Homeland Security (DHS)-owned patent applications and patents available for licensing can be found at **vps.labworks.org**
Commercialization Accelerator Program (CAP)	CAP increases the likelihood of successful transfer of federally funded technologies from lab to market **www.dhs.gov/science-and-technology/cap**
Cooperative Research and Development Agreements (CRADAs)	DHS CRADAs facilitate collaborative R&D activities between DHS and non-federal entities. S&T executes CRADAs across DHS to support the development and delivery of technology solutions to homeland security end users **www.dhs.gov/science-and-technology/cradas**
Homeland Security Startup Studio (HSSS)	Pairs teams of entrepreneurs with promising federally funded technologies to assess their commercialization potential and move the technologies to market **www.dhs.gov/science-and-technology/homeland-security-startup-studio**
Partnership Intermediary Agreements (PIAs)	Non-profit entities with specialized skills to assist DHS with technology transfer and commercialization activities **www.dhs.gov/science-and-technology/technology-transfer-partnership-intermediaries**
HSWERX	Fostering collaboration to enable the rapid discovery and acceleration of innovative solutions that meet homeland security needs. **www.dhs.gov/science-and-technology/HSWERX**

DOING BUSINESS WITH THE FEDERAL GOVERNMENT AND DHS

FEDERAL PROCUREMENT

Acquisition Planning Forecast System

The Acquisition Planning Forecast System is a searchable database geared toward small businesses. It projects all anticipated contract actions above $250,000 that small businesses may be able to perform, either through a direct contract with DHS or through a subcontract arrangement with a prime contractor. Procurements valued under $250,000 are not listed; businesses are urged to contact the appropriate DHS Small Business Specialist for each Component for information on those opportunities. **apfs-cloud.dhs.gov**

Grants

The Government Acquisition & Grants Portal helps more than 100,000 vendors and grant applicants find, respond to, and win opportunities for contracts, grants, and other types of assistance funding. Grants.gov houses more than 1,000 grant programs and vets grant applications for federal grant-making agencies. **www.grants.gov/**

Registration

The federal government has centralized business information in a one-stop platform called www.usa.gov/business, aimed at making it easier for businesses to access services to help them grow and hire. If you want to do business with the federal government, there are rules and procedures to follow to qualify. For further help, see **www.usa.gov/business**

SAM.GOV

SAM.gov is the single point-of-entry for federal government procurement opportunities over $25,000. Through one portal— SAM.gov–government buyers directly publicize their business opportunities, and commercial vendors seeking federal markets for their products and services can search, monitor, and retrieve opportunities solicited by the entire federal contracting community. Doing business with the federal government starts with registration, which requires you to obtain a Unique Entity ID from **SAM.gov** for administrative, contracting and tax purposes.

Sub-contracting with Prime Contractors

Large business prime contractors at DHS may be interested in subcontracting with small, minority, women-owned, HUBZone-certified, 8(a), veteran-owned, and service-disabled businesses. The DHS list of prime contractors provides visibility to pursue this avenue toward contracting work. **www.dhs.gov/prime-contractors**

Small Business Contracting Assistance Programs

The U.S. Small Business Administration has resources to specifically help small businesses and entrepreneurs navigate federal procurement opportunities. Geared toward specific sub-sets of business owners, these programs help small businesses through mentorship and exclusive contracting opportunities. **www.sba.gov/federal-contracting/contracting-assistance-programs**

Teaming and Subcontracting Opportunities with IT Contracts

DHS is establishing Department-wide contracts for information technology (IT) services and commodities. For the latest on IT task orders and teaming and subcontracting opportunities, see **www.dhs.gov/information-technology-acquisitions**.

Unsolicited Proposals

If you do not find a current open opportunity through S&T, you may consider submitting your capability through the DHS Unsolicited Proposal Process. This process is for innovative and unique products and services that are not commercially available, and specific criteria must be met before an unsolicited proposal can be submitted. Find out more at **www.dhs.gov/unsolicited-proposals** to begin this process.

Additional Resources

DHS provides additional online resources where businesses can find contract opportunities at **www.dhs.gov/how-do-i/for-businesses**.

CONNECT WITH US

Connect with us and keep up to date on the latest S&T news and opportunities!

LEARN MORE ABOUT WORKING WITH US

www.dhs.gov/science-and-technology/work-with-st

FIND OUT ABOUT OUR EVENTS

www.dhs.gov/science-and-technology/engage-st

SIGN UP FOR S&T'S PARTNERSHIP CONNECTIONS AND PROGRAM MAILING LISTS

https://go.dhs.gov/JUA

EMAIL US AT
SandT.Innovation@hq.dhs.gov

FOLLOW US ON X
@dhsscitech

LIKE US ON FACEBOOK
dhsscitech

FOLLOW US ON LINKEDIN
DHS Science and Technology Directorate

SUBSCRIBE TO OUR CHANNEL
DHS Science and Technology Directorate

FOLLOW US ON INSTAGRAM
@dhsscitech

BORDER SECURITY

DHS secures U.S. borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems. S&T invests in border security research and development for technologies and solutions to prevent illicit movement and the illegal entry or exit of people, weapons, dangerous goods, and contraband; and provides solutions that help manage risks posed by people and goods in transit.

Air, Land, and Port of Entry (POE) Security

Technical capabilities are needed to strengthen the security of our national airspace and land border by detecting and preventing the flow of illicit goods and people, while also facilitating and safeguarding lawful trade and travel through ports of entry.

Air Security

CHALLENGE: DHS operational elements, law enforcement, and first responders must maintain persistent air-domain awareness of all manned and unmanned aircraft in the national airspace to identify anomalies in patterns, connect disparate events, and detect potential threats. Converging mission requirements, emerging asymmetric threats, evolving technologies, and critically strained resources require advanced technologies that produce efficient, force-multiplying aerospace coverage. These technologies include sensors to detect, track, and classify manned and unmanned aircraft; intelligence, surveillance, and reconnaissance sensor technology with command and control and advanced air mobility; communications tools for disseminating time critical and operationally relevant information from air-based platforms; and tools to improve operational efficiency and reduce the lifecycle costs of operational technologies.

IMPACTS: ICE, CBP, USCG, and first responders at the local, county, and state levels will be able to cost-effectively invest in aircraft technologies, sensors, small unmanned aircraft systems (sUAS), and ground-control equipment that will meet mission needs, integrate into ongoing operations, and address privacy and safety concerns.

Trade and Commerce Protection

CHALLENGE: CBP needs to leverage technology to safeguard the American public and promote legitimate international commerce while considering the increasing volume and complexities of international trade. This includes enhanced capabilities to enforce trade laws against counterfeit, unsafe, and fraudulent inbound goods and to facilitate lawful trade. CBP also requires technology assistance on advanced analytics and machine learning (ML).

IMPACTS: Meeting the challenges in this area will result in the expedited processing of legitimate commerce and will enhance CPB's abilities to target illegal or fraudulent cargo; efficiently collect duties, taxes, and tariffs; and effectively enforce U.S. trade law.

Ground-Based Technologies

CHALLENGE: DHS components need capabilities to reliably and accurately detect, identify, classify, track, and interdict illegal activity along land borders and via telecommunications networks around and between POEs. Commercial telecommunications companies are deploying new networks that may pose challenges to law enforcement investigators who use digital tools to locate and investigate criminal and terrorist activity on telecommunications networks.

IMPACTS: Meeting the technology challenges will enhance land-domain awareness, increase detection and tracking of illicit border activity, facilitate data sharing and analytics to support CBP and ICE investigations, increase the interdiction of illicit border activity, enhance the effectiveness of field agents, and provide new tools and methods to investigate and prosecute suspected criminals and terrorists.

Data Visualization and Emerging Analytics

CHALLENGE: CBP needs data visualization and emerging analytics that can enhance tracking for cargo and people from origin to destination with advanced interactive visual analytics to better identify transnational activity and provide additional insights into customs recovery and threat detection in the supply chain while expediting trade.

IMPACTS: Enhanced tools for visualizing and analyzing transportation data will facilitate CBP's ability to identify, investigate, and prosecute illegal activity related to the transport of illegal goods and people across U.S. borders.

Tunnel Detection and Surveillance

CHALLENGE: CBP and ICE need capabilities to reliably detect cross-border tunnels, support unmanned investigations of discovered tunnels, and perform forensic analysis of tunnels to support investigations and prosecutions.

IMPACTS: New technical solutions to safely detect and investigate tunnels will increase CBP's ability to investigate and exploit discovered tunnels, facilitate the arrest and prosecution of individuals involved in creating and using the tunnels, and prevent hundreds of tons of drugs from reaching U.S. streets.

International Mail

CHALLENGE: In accordance with legislative requirements to identify and prevent illegal imports, CBP needs to inspect hundreds of thousands of pieces of incoming international mail each day to prevent prohibited items from entering the United States. CBP needs improved processes and technologies to facilitate and expedite the inspection of incoming international mail.

Impacts: Upgrading the related equipment and technologies will enhance CBP's ability to interdict illegal or fraudulent mail and improve the efficiency of collecting duties, taxes, and tariffs.

Non-Intrusive and Alternate Inspection Technologies

CHALLENGE: CBP's non-intrusive inspection systems need technology improvements to maintain parity with emerging threats. Although the volume of inbound goods and people passing through the POEs is projected to increase from year to year, CBP manpower will not increase proportionately. Therefore, CBP requires improvements in software algorithms, ML, and threat detection to enhance efficiency and expand the range of detectable threats.

IMPACTS: Upgrading equipment, software, and processes will increase interdiction rates, increase the throughput, and improve resource loading to provide a significant increase in efficiency without additional staffing.

Biometrics and Identity Management

Biometric and other identity technologies facilitate identity inspections and screening operations across U.S. POEs, transportation security checkpoints, secure facilities, and online systems. Data-driven approaches help identify and prioritize changes in existing operations based on anticipated improvements, consequences, and costs of new solutions.

Biometrics and Identity Screening

CHALLENGE: DHS components require more efficient identity and biometric capabilities to improve screening and the identification of people accessing secure federal facilities and those who are arriving in, departing from, and traveling within the United States. Improving the accuracy, flexibility, and scalability of these capabilities must balance security concerns with ongoing needs to facilitate lawful trade and travel.

IMPACTS: Updated capabilities will result in enhanced, less intrusive traveler identification validation; improved abilities to detect terrorists, criminals, and dangerous individuals; streamlined, scalable, and cost-effective security, screening, and inspection operations; reduced technical risk in DHS's acquisition of secure, interoperable, enterprise solutions; improved DHS staffing efficiency; and improved traveler throughput and satisfaction.

Counter Unmanned Aircraft Systems

Research, test, evaluate, and transition technical capabilities that strengthen the security of DHS-designated and -approved covered assets and facilities by detecting, tracking, identifying, and mitigating the threat posed by nefarious sUAS.

Counter Unmanned Aircraft Systems (C-UAS)

CHALLENGE: Recent technology advances have resulted in inexpensive and easily obtainable sUAS for a variety of uses, some of which are nefarious. DHS is responsible for protecting critical infrastructure and certain facilities and assets from nefarious UAS use. DHS needs improved technology and equipment to identify DHS component operational requirements based on their specific mission sets, identify potential commercial off the shelf (COTS) and Government off the shelf (GOTS) solutions that meet component operational requirements, and apply COTS, GOTS, and other mature technologies to address urgent needs. S&T must coordinate with Department of Transportation (DOT)/Federal Aviation Administration (FAA) to ensure minimal impact to the National Airspace. S&T needs to conduct rapid test and evaluation of technologies in support of component acquisitions.

IMPACTS: Meeting the complex challenges in this category will result in well-defined and validated DHS component C-UAS requirements and acquisition strategies, knowledge of the state of the sUAS market and existing COTS and GOTS C UAS systems, and solutions to meet component-specific requirements.

Forensic and Criminal Investigations

Multiple DHS components are tasked with the detection and investigation of various types of criminal activities. To maintain effectiveness and the ability for quick action requires technology, procedures, and intelligence capabilities that enable DHS components to collect, analyze, share, and act on law enforcement data and information.

Digital Forensics

CHALLENGE: Law enforcement officials in various agencies need fast, intelligent technology and tools to combat the explosion of online child sexual exploitation. The current manual process is slow and labor intensive. Law enforcement agents need automated technology to sort and analyze the massive amounts of digital images and data to locate crime scenes, identify and rescue victims, and identify and apprehend perpetrators.

IMPACTS: Speeding up triage and improving the efficiency and accuracy of the forensic deep-dive analysis of seized exploitive digital imagery will shorten the time to rescue victims, provide evidence for prosecution, and reduce agents' exposure to traumatizing material. New digital forensics tools developed for the child exploitation problem could be leveraged for other crimes with digital evidence.

Illegal Immigration Investigations

CHALLENGE: DHS is securing the U.S. border and executing the Centers for Disease Control and Prevention's (CDC) public health authority to safeguard the health of the American public and migrants, and protect children. ICE is working around the clock to process the flow at the border, collaborating with other agencies in an all-government effort to address the current situation at our southwestern border, and seeking longer-term solutions to irregular migration from countries in our hemisphere that are suffering worsening conditions.

IMPACTS: Upgrading systems, proving technology solutions, and implementing methods for humanely enforcing immigration laws will facilitate ICE and Enforcement and Removal Operations in their implementation of immigration processes and help prevent the need for detention.

Transnational Organized Crime and Counter Networks

CHALLENGE: Efforts to combat transnational organized crime (TOC) are currently hampered by the growing online presence of these networks and actors and the difficulty of detecting and preventing criminal behavior. DHS components require connected, purpose-built data systems and forensic tools that enable enterprise-wide data sharing and a centralized data-analytics platform to facilitate and encourage collaboration across DHS components.

IMPACTS: Component efficiency and effectiveness will be enhanced by implementing an upgraded, unified approach to combatting TOC. Centralized data hosting and analytics, distributed access to a collaboration platform, and vital new forensic tools that incorporate artificial intelligence (AI) and ML will allow agents from disparate agencies to share discoveries, theories, and analysis and improve the performance of these tools for law enforcement applications.

Immigration Services

USCIS is responsible for adjudicating all applications and petitions for immigration benefits; maintaining the cohesiveness of legitimate immigration IT systems; and providing trust-worthy and timely immigration, employment, and identity information.

Immigration-Based Technologies

CHALLENGE: USCIS needs to improve the efficiency and guarantee the integrity of immigration services and activities to reduce the lengthy applicant backlog. Meeting this challenge includes upgrading the technology and related processes used for the adjudication of citizenship and other immigration applications to strengthen and streamline the vetting process.

IMPACTS: Upgrading computers and software will enhance USCIS's ability to efficiently process immigration benefit applications and petitions, identify fraudulent immigration applications and petitions, reduce applicant backlogs, and improve customer throughput and satisfaction.

Maritime Safety and Security

U.S. maritime border-security agencies and service bodies safeguard lawful trade and travel to prevent the illegal transport of illicit goods or people and maintain the safety and resilience of the maritime transportation system.

Port and Coastal Surveillance

CHALLENGE: USCG, ICE, and CBP require operational capabilities to improve maritime domain awareness (MDA); enhance their ability to detect, deter, interdict, and investigate illegal maritime activity; and coordinate across the HSE. This includes sensors and platforms (including autonomous systems), information-sharing technologies, mission support tools and techniques, and decision-support capabilities.

IMPACTS: Enhanced, automated, and well-connected technologies for MDA would support the abilities of all related agencies to detect, track, and interdict illicit activity; increase the efficiency, effectiveness, and safety of personnel and equipment; augment U.S. presence in the maritime domain; and enhance and automate information-sharing to support DHS maritime safety and security missions.

Port and Waterway Resilience

CHALLENGE: The USCG needs upgraded tools to conduct rapid and accurate port and waterway health assessments, analyze the condition of ports or waterways after incidents or disasters, and develop risk-based approaches for mitigation, response, and recovery. These tools include support for analytical visualization, measurement and data collection, and other more effective and user-friendly capabilities that support maintaining resilience of ports and waterways.

IMPACTS: Upgrading and supplementing these technologies will help ensure human and environmental safety, preserve the economic security of maritime ports and waterways, improve situational awareness and understanding of waterway criticality, and enable decision-making for more efficient and effective resource allocation to keep ports and waterways open.

Remote Maritime Operations

CHALLENGE: USCG and CBP need to operate in the Arctic and other remote maritime regions and effectively detect and respond to illicit maritime activities, hazards, or emergencies in a timely manner.

IMPACTS: Upgraded, remote, and autonomous monitoring equipment will reduce risks to staff and equipment while enhancing capabilities for near real-time detection of illicit activities or emergency situations in the Arctic and other remote regions; real-time analytics at scale; time-dominant operations; and while responding to illicit maritime activities, hazards, and/or emergencies.

CHEMICAL, BIOLOGICAL, AND EXPLOSIVE (CBE) DEFENSE

S&T supports prevention, protective strategies, and the coordinated surveillance and detection of CBE threats. S&T's R&D efforts focus on the creation and improvement of technology, methods, and procedures for detecting CBE threats including the prevention of terrorism; reduction of critical infrastructure vulnerability from terrorist attacks and other hazards; and detecting and preventing the illicit movement and illegal entry or exit of people, weapons, dangerous goods, and contraband.

Chem-Bio Detection

DHS components assess, prepare for, prevent, detect, respond to, and recover from incidents involving chemical and biological (CB) threats and hazards. DHS and the HSE use risk-awareness tools, knowledge products, and technical solutions to protect the nation from incidents involving CB hazards and to counter CB threats. A rapid response to CB events (biological or chemical attacks or a disease outbreak) is critical to save American lives, protect critical infrastructure, and safeguard the U.S. economy.

Chem-Bio Threat Surveillance

CHALLENGE: Providing timely, effective, and accurate surveillance methods in enclosed spaces is essential for the prompt detection of threats and the subsequent coordination and rapid response actions that must occur. DHS components; other federal agencies; and state, local, tribal, and territorial (SLTT) customers, including public health and first responder communities, depend on the effectiveness, accuracy, and accessibility of surveillance infrastructure for the timely detection of and confident response to the release of and/or exposure to harmful chemicals and biological pathogens. Aging systems and software and a worsening threat environment are hampering component abilities to detect threats and coordinate and communicate effective safety and countermeasures.

IMPACTS: Updated technology and tools and cost-effective capabilities for detecting, communicating, and responding to biological and chemical threats will help responsible DHS components prepare for, potentially prevent, and respond to these threats and save the lives and health of those affected in an attack.

Food, Agriculture, and Veterinary Defense

CHALLENGE: The United States is at risk for outbreaks of highly infectious and dangerous foreign animal diseases—which can be introduced to the United States through natural, accidental, or deliberate means and can spread within the U.S. agricultural system causing major economic disruption to the agriculture sector and the health of the human population. Mitigating these risks requires next-generation vaccines and other countermeasures to ensure that the U.S. Department of Agriculture (USDA) and other first responders have the information and tools needed to effectively identify, respond to, and recover from foreign animal disease outbreaks.

IMPACTS: Strengthening the defense of the U.S. agricultural infrastructure to ensure that USDA and other first responders in the animal agriculture community have effective responses to foreign animal disease outbreaks. Multi-pathogen countermeasures would provide faster and more comprehensive protection to limit the spread and size of an outbreak. Improved data would support the regulatory licensing and/or availability of new countermeasures in the event of a high-consequence outbreak in the United States.

Multifunction Detectors

CHALLENGE: DHS components and SLTT first responder communities currently use multiple technologies to detect or confirm different categories of threat agents, creating logistical and operational challenges. To streamline the detection and identification of chemical and biological threats, DHS agents need a handheld system that can accurately and simultaneously detect and identify a broad range of threats in a variety of environments.

IMPACTS: A single, handheld device with multifunction bio-chemical hazard detection and identification technologies would allow DHS personnel to execute an efficient, integrated approach to CB security and defense; provide rapid, reliable interdiction of CB hazards; and increase the safety, situational awareness, timeliness, and reliability of hazard detection and response for front-line operators.

Wide-area Decontamination

CHALLENGE: A terrorist attack involving the release of an aerosolized biological agent in a major metropolitan area, often located along a coastal region or inner waterway, will require field-tested methods to rapidly restore vital services and critical infrastructure necessary to serve and help protect the public. These services and technologies include effective and scalable methods for characterization, decontamination, waste management, and the clearance of wide-area biological agents.

IMPACTS: Providing effective and efficient methods for rapid recovery of large metropolitan regions, coastal areas, and critical government assets following a wide-area biological contamination event will enable faster re-occupation of populated areas and restore confidence in the safety of natural resources (e.g., drinking water).

Urban Security

CHALLENGE: Subway systems, other mass transit systems, and indoor venues that serve large metropolitan areas are attractive targets for potential acts of bioterrorism, particularly with aerosolized biological threat agents. New chemical and bio-detection technologies, detection architectures, and mitigation strategies are needed to limit agent transport and public exposure to an aerosolized threat.

IMPACTS: Improved detection and neutralization tools and techniques would minimize the impact and consequences of a bioterrorism event in underground and above-ground mass transportation systems and indoor environments.

Detection Canine Services

Detection canines are a valuable resource in responding to new and emerging threats including drugs of various kinds, existing and newly identified explosive materials, and occurrences of global human pandemics such as COVID-19.

Detection Canine Skills and Efficiencies

CHALLENGE: Improving the operational proficiency of over 16,000 detection canine teams requires new tools, techniques, and knowledge to better understand, train, and employ detection canines and their handlers. Over the last 20 years, the demand for elite detection canines from foreign countries has increased while domestic supply has not kept, pace resulting in a subsequent reduction in the quality of available canine candidates.

IMPACTS: Expanding the domestic detection canine supply and developing more effective canine-handler training techniques will improve detection canine proficiency in operational environments, provide more reliable responses to emerging biological and chemical threats, and address the growing threat and operational concerns of securing soft target venues and large public events.

Opioid/Fentanyl Detection

DHS components and law enforcement partners use advanced detection and intelligence capabilities to enable the confident discovery and interdiction of opioids and other narcotics being smuggled across U.S. borders without disrupting the flow of legitimate commerce.

Opioid/Fentanyl Detection

CHALLENGE: DHS needs to disrupt the flow of synthetic opioids like fentanyl that cross U.S. land, sea, and air borders. Specific needs include physical detection and interdiction of synthetic opioids smuggled in very small or dilute quantities; automated detection systems; and discovery and disruption of TCOs, drug trafficking organizations, criminal networks, and individuals who exploit open source and dark web marketplaces to support illicit manufacturing and smuggling. DHS components and law enforcement partners have identified critical needs for advanced technologies to aid in their missions to target, investigate, and dismantle illicit opioid and other narcotic smuggling into the United States.

IMPACTS: Providing DHS components and law enforcement partners with advanced, operationally effective detection and intelligence capabilities will enable the confident discovery and interdiction of opioids and other narcotics being smuggled across U.S. borders without disrupting the flow of legitimate commerce.

COUNTER TERRORISM

S&T works to identify individuals or groups that intend to conduct terrorist attacks and/or illicitly move weapons, dangerous goods, and contraband. It also provides assessments of high-consequence attack methods such as CBE threats that terrorists may use to attack the United States.

Emerging Risks and Technologies

S&T supports DHS operational missions by conducting assessments, studies and analyses to identify and prioritize emerging risks and technologies, including determinations of adversarial use and representing opportunities to use and opportunities to mitigate the adverse impacts of emerging technologies to protect the Nation.

Emerging Risks and Technologies

CHALLENGE: DHS needs to identify, contextualize, and prioritize critical emerging risks and leverage emerging technologies to defend against them. Trends, risks, and opportunities must be identified as far in advance as possible in collaboration with government agencies, partners in the defense and intelligence communities, and the private sector. Versatile technological solutions that can address a wide range of areas or be easily tailored to changing needs will ensure readiness and provide efficient, cost-effective tools.

IMPACTS: More reliable emerging risk assessment will facilitate the prioritization of response strategies across critical DHS missions. The collection and analysis of key metrics involving antagonistic trends, eroding infrastructure, and fragile ecosystems will enable DHS to determine its posture toward emerging risks; communicate with interagency, academic, industrial, and international communities; and focus resources and investments to best meet mission requirements.

Explosives Threat Assessment

S&T researches and identifies current and potential explosive threats to understand the risk posed to the United States, bolster the international aviation security system, improve various security processes and technologies, and encourage partnerships with industry. These responsibilities encompass risk-based threat characterization, attribution, strategic planning, explosive magnitude disaster potential, and employ a range of analytical technologies, strategies, and procedures.

Aircraft Vulnerability

CHALLENGE: DHS needs to understand the vulnerability of commercial aircraft to the broad range of conventional and emerging improvised explosive device (IED) threats, including the vulnerability of new composite aircraft structures currently entering the civil transport fleet. When designing screening technologies for the detection of explosives on passengers, in checked bags, or in air cargo, the agency must determine the effects that explosive threats have on commercial aircraft.

IMPACTS: Providing TSA the information required to ensure that the explosive detection system's threat thresholds are sufficient to prevent introduction of explosive threats that would result in catastrophic aircraft loss if detonated, will help reduce the vulnerability of commercial aircraft to internal explosive threats.

Homemade Explosives (HMEs)

CHALLENGE: Detonation of an HME device presents an ongoing threat to the public using transit services and in public places. DHS needs to better understand and address the persistent and continuously evolving threats from HMEs. This requires research, development, integration, and certification testing for the identification, detection, and mitigation of threats, including the management and use of laboratory facilities.

IMPACTS: Providing TSA and other DHS components with better technology and facilities that will allow the agency to develop and field more effective transportation security equipment, provide better training to frontline personnel, validate and monitor continuing and emerging threats, and transition products to protect national security and build resiliency.

Technology Explosives Assessment

CHALLENGE: Rapidly evolving explosive threats complicate the ability of current TSA screening approaches to detect new threats as they emerge. DHS needs tools and approaches for rapidly characterizing these evolving and emerging explosive threats and to drive the development and validation of versatile screening equipment to reliably detect new and emerging threats.

IMPACTS: Availability of faster, more accurate, and more cost-effective threat-screening equipment that conforms with TSA's requirements for detecting existing and emerging explosive threats, and a process to drive innovation and foster the development of new technologies for detecting other contraband substances (e.g., opioids).

Probabilistic Analysis of National Threats, Hazards, and Risks (PANTHR)

S&T, DHS components, and the HSE address biological, chemical, and hazard knowledge gaps to inform defensive strategies that provide accurate, useful, and defensible knowledge and tools to decision makers in time to enable informed choices for defense against threats and attacks. Advanced, tailored analysis capabilities, tools, and processes are required to support national threat assessments, characterize biological and chemical hazards, develop effective and targeted biological and chemical defenses, and coordinate hazard awareness and characterization activities across populations.

Chemical and Biological Threat Characterization

CHALLENGE: DHS components require updated analytical tools, data, and processes to provide more accurate and timely predictions of the risks and consequences of chemical and biological attacks. Substance characterization data and advanced analytical tools and processes are also needed to define performance requirements for defensive countermeasures (e.g., detectors, personal protective equipment, and operational protocols) to develop solutions that effectively mitigate hazards posed by chemical and biological threat agents.

IMPACTS: Improved, rapidly available characterizations (data) of chemical and biological agents will inform advanced analytical processes and produce knowledge products that will enhance decision-makers' abilities to effectively prioritize defense investments to prevent, prepare for, respond to, and recover from an attack based on the specific nature of the deployed substance.

Integrated Risk Evaluation

CHALLENGE: DHS decision-makers need relevant risk data that characterize the likelihood of threats from weapons of mass destruction to manage resources and reduce the likelihood and impact of chemical, biological, radiological, and nuclear (CBRN) incidents. Current tools and processes do not meet the requirements for efficient targeted, coordinated, cohesive surveys of the current threat environment and our ability to prevent or mitigate damage in specific at-risk locales.

IMPACTS: Improvements and additions to the existing risk-evaluation toolset and process will enable efficient, tailored analyses that assess chemical and biological risks and enable strategic, operational, and tactical decisions to increase prevention, protection, preparation, mitigation, response, and recovery from CBRN hazard events. Better assessment of potential threats and greater understanding of hazards enables improved risk management and bolsters DHS's abilities to prioritize resources based on the highest potentials for occurrence and damage.

CYBERSECURITY AND INFORMATION ANALYSIS

The increasing reliance on complex data, technology, communication, and interconnectivity has expanded arenas of potential vulnerabilities and increased potential risk to governmental, citizen services, and critical infrastructure continuity. Protecting individuals and organizations from cyberattacks requires R&D, test and evaluation, and the technology transition of advanced cybersecurity and information assurance technology solutions to secure current and future critical cyber infrastructure.

Cybersecurity

AI/ML, data analytics, cyber analytics, natural language processing, and software assurance all play important roles in securing industrial control systems, information related to all aspects of life, and communication networks. Fully researched and vetted technologies designed to strengthen defensive cybersecurity capabilities in a spectrum of strategic technical areas will mitigate risk to U.S. critical infrastructure, federal agencies, and SLTT organizations.

Cybersecurity, Artificial Intelligence, and Machine Learning

CHALLENGE: The growing threats to national, organizational, and personal information and cyber infrastructure create vast, complex risks that cannot be managed with traditional approaches or outdated technology. The CISA needs AI and ML applications to automate and streamline advanced analytics.

IMPACTS: Providing applied AI and ML infrastructure, algorithms, and tools will enable security orchestration, automation, and response; behavioral anomaly detection; data reduction; tipping and queuing of analyst workflows; and other user-driven mission needs.

Data Analytics Collaborative Environments

CHALLENGE: Working collaboratively to build efficiency, manage resources, and minimize discrepancies requires a centralized source and capability that will allow operational units to query and correlate information related to cyber risk analysis, physical and infrastructure risk, and blended cyber-physical risks and threats.

IMPACTS: A secure, centralized data platform would allow CISA to correlate the data collected from all CISA programs into a common information architecture available to all CISA critical mission activities. The related hybrid cloud infrastructure would support the full breadth of cyber defense operations, encryption techniques, and commercial solutions to enable sensitive, unclassified data sharing with critical infrastructure owners and operators. The centralized platform and infrastructure would protect privacy, application programming interfaces, and data access mechanisms to ensure that data is available within and across CISA and mission partners.

Cyber Analytics Tools and Techniques

Challenge: Currently, malware analysis relies largely on time-consuming, manual processes. CISA needs improved computational analytics and information-sharing facilities to improve DHS cyber-physical security risk analysis and encourage collaboration across government agencies to improve process efficiency.

IMPACTS: Advanced cyber analytic capabilities, including AI, ML, and natural language processing (NLP) would facilitate automating malware analysis, leverage expertise across multiple partners to accelerate cyber-related R&D, use data and analytics to gain information about adversaries and improve real-time network defense, and upgrade and improve existing risk assessment methods that are needed to develop the National Critical Functions risk architecture.

Natural Language Processing Capabilities

CHALLENGE: The emerging cyber-physical landscape has opened new avenues to malicious incursions of physical infrastructure, from manufacturing equipment to home appliances. CISA's traditional security products (alerts, warnings, assessments) are not sufficient to detect or deter cyberattacks on our physical infrastructure and devices. CISA needs NLP algorithms, approaches, and technologies to better correlate CISA's heavily structured cyber data with its unstructured physical infrastructure security data.

IMPACTS: NLP and ML algorithms can ensure alignment with CISA's Enterprise Conceptual Data Model, populate required metadata, and improve the results of CISA's security alerts, warnings, and assessments.

Software Assurance

CHALLENGE: CISA works to ensure that software applications relating to security and safety in government environments are free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle. The agency needs enhanced cybersecurity tools and analytic techniques to detect malicious and problematic software sooner in the software development lifecycle, potentially preventing our adversaries from compromising critical systems.

IMPACTS: Enhanced software assurance tools and processes that can quickly and reliably analyze software to determine which aspects of an organization's code base are least mature and need attention, and analyze software composition of codes at the source, byte, and binary levels to track usage, origination, and identify extra features that are not needed.

Industrial Control Systems and Cyber-Physical Security

CHALLENGE: CISA and critical infrastructure operators are hampered in their efforts to prevent inadvertent errors or malicious actions from negatively affecting various industrial and manufacturing control systems. System and network monitoring capabilities are required to immediately identify negative impacts to process safety, function, or efficiencies, and improve defensive capabilities to negate or minimize impacts.

IMPACTS: Identifying weaknesses and installing and upgrading operational technology networks, industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) monitoring and other defensive measures (e.g., intrusion detection and prevention systems, agent-based security mechanisms, and automated patch management capabilities) will help protect national critical infrastructure.

Communications Security

CHALLENGE: The security risks associated with cellular networks include network operations, stakeholder data protection, and supply chain management. Research and applied solutions are needed to ensure the security of the communications ecosystem from mobile devices, software applications, and data to the underlying infrastructure of carrier networks, mobile operating system providers, and enterprise systems and infrastructure.

IMPACTS: Enhancing the interoperability and integrity, reliability, and security of critical communication systems for DHS components through the promotion and use of standards-based solutions.

FIRST RESPONDER / DISASTER RESILIENCE

Improving the United States' ability to withstand, respond to, and recover from disasters and hazardous situations of all kinds, regardless of the cause, is becoming increasingly important due to the increase of possible threats from foreign adversaries, our eroding infrastructure, rising inter-community hostility, and fragile environments.

DHS's goals in this area include reducing the vulnerability of critical infrastructure to terrorist attacks and other hazards by working with SLTT and local governments to secure their information systems and identify hazards and assess vulnerabilities; by developing strategies to manage risks, increase the level of disaster preparedness of SLTT partners, nongovernmental organizations, the private sector, and the general public; by improving emergency and interoperable communications capabilities; and by improving the emergency management and leadership capabilities of DHS and its components.

Cargo, Baggage, and People Screening

Transportation systems need advanced, versatile screening systems to detect threats to the safety of passengers and vehicles. The development of prototype solutions to bridge technology capability gaps within the security screening processes will help ensure the safety of air travel and other mass transportation systems.

Air Cargo Screening

CHALLENGE: DHS needs next generation air cargo screening systems to address challenges posed by the increasing volume of air cargo and the wide range of air cargo commodity types. Evolving threats contained in air cargo pose a significant and continual threat to passenger safety. Process and technology needs include augmenting existing screening systems via advanced hardware and software, developing low-cost computed tomography (CT) systems for 3D imaging of skids, automated threat detection algorithms, and technologies to screen dense cargo.

IMPACTS: Providing next generation cargo screening capabilities will strengthen the air cargo and aviation security infrastructure, which has a vital impact on passenger safety and economic interests.

Next Generation Explosives Trace Detection

CHALLENGE: DHS needs enhanced explosives screening at aviation checkpoints, border crossings, and large public events. National security forces, the end users of explosive trace detection technologies, need more effective tools to detect, identify, and confirm emerging explosive threats. S&T must continue to assess the effectiveness of deployed technologies against emerging threats; identify capability gaps; develop capabilities to address these gaps; and test, evaluate, mature, and transition these capabilities to end users.

IMPACTS: Providing knowledge and capabilities to meet evolving explosive threats and equipping end users and operators with the equipment and tools needed to optimize operations and keep false alarm rates low will reduce passenger wait times and the need for agent contact.

Primary Screening for Carry-On Baggage

CHALLENGE: As the number of travelers with carry-on bags increases and as new threats emerge, TSA needs next generation technology for screening carry-on bags to meet the increased demand, optimize operations, keep false alarm rates low, and enhance end-user satisfaction by reducing wait times and the need for agent intervention.

IMPACTS: Providing TSA with advanced technology will facilitate greater throughput and higher security measures and reduce operator burden. Improved technologies and algorithms would allow TSA to detect prohibited items quickly and accurately without removing electronics, liquids, aerosols, powders, or gels.

Primary Screening for Passengers

CHALLENGE: As the number of travelers increases and as new threats emerge, TSA needs next generation passenger screening technology to meet increased demand, optimize operations, keep false alarm rates low, and enhance end-user satisfaction by reducing wait times and the need for agent intervention.

IMPACTS: Providing advanced checkpoint technologies will provide faster, less invasive, and less costly screening of passengers. Limited requirements for passengers to remove items will decrease passenger inconvenience and increase checkpoint throughput. Systems with material discrimination ability will determine if suspect items are potentially harmful or benign, reducing the need for pat-downs and other intrusive security measures.

Checked Baggage Technology

CHALLENGE: TSA needs next generation checked baggage screening technology to optimize operations, minimize false alarms, and automatically detect the full array of existing and emerging explosives and non-explosive contraband materials. Additional needs include an expanded library of detectable explosives and explosives signatures; enhanced threat image projection tools to improve efficiency; improved system reliability, screening speed, and reduced cost; and improved baggage movement technologies that support changes to security parameters to improve operations and allow for innovative infrastructure solutions.

IMPACTS: Providing TSA with enhanced threat detection capabilities, lower false alarm rates, improved alarm resolution, and reduced lifecycle costs will allow TSA to keep pace with new threats and the evolution of the traveling public.

Screening at Speed (SaS)

CHALLENGE: Current TSA airport checkpoints are costly and time-consuming to upgrade in response to evolving threats, subject to false alarms that require intrusive pat downs and manual searches to resolve, and require passengers to remove personal belongings. TSA needs detection technologies that effectively and efficiently screen for concealed threats using an integrated system-of-systems with layered screening technologies.

IMPACTS: Providing integrated screening tools with real-time and walk-by sensing, wide-area surveillance, credential authentication, risk-based screening, and other technologies will reduce overall risk throughout in airports and in other operational areas including soft targets and special national security events. Improved detection probabilities and reduced false alarms will translate into fewer secondary inspections, lower per-passenger costs for TSA, and reduce passenger inconvenience. A system-of-systems approach integrated using open architectures and capable of deploying a layered aviation security posture from curb-to-gate will reduce security risks and costs and facilitate rapid, cost-effective system upgrades to continue countering evolving adversaries.

Community and Infrastructure Resilience

Protecting at-risk communities and infrastructure includes the involvement of state, local, and the private sector in plans and recommendations as well as investigating new and emerging technologies for streamlining and optimizing FEMA disaster resilience investments in insurance, mitigation, and recovery operations.

Climate Adaptation and Resilience

CHALLENGE: Climate change directly impacts the DHS mission; the nation faces increased loss of life, infrastructure damages, and economic costs due to natural disasters driven by climate change. These increases impact the ability of the federal government to financially support disaster recovery and develop and maintain a sound financial framework for the National Flood Insurance Program (NFIP).

Impacts: Identifying affordable, game-changing technologies such as self-healing materials and other innovations can protect the American people from the impacts of worsening climate conditions such as droughts, flooding, wildfires, and hurricanes.

Disaster Recovery

CHALLENGE: Local communities need access to new and emerging technologies and innovations to streamline and optimize disaster recovery operations and assistance programs. Communities need to expedite recovery and reduce the time necessary to restore critical functions, establish community lifelines, and assist survivors in getting back to their daily lives.

Impacts: Identifying and implementing new technologies for disaster recovery will help expedite recovery assistance to survivors and households in affected communities, track and monitor restoration functions through improved damage assessments, reduce the complexity of applying for and receiving assistance, promote adaptive recovery, and enable faster decision-making.

Flood

CHALLENGE: New and emerging technologies are needed by FEMA and state and local governments to identify high-risk areas for remediation, predict and alert impending floods, and reduce future fatalities and damage. Needed processes and technologies include new flood sensors and alerting systems, smarter remote sensing for situational awareness, new analysis products using high-performance computing and AI, realigned economic incentives and risk analysis, enhanced community resilience, improved access to high-quality flood data, and improved predictive models and analytic services.

IMPACTS: Better flood risk analysis through more effective use of existing data sources to create multi-dimensional representations of community functions using an integrated system-of-systems approach. Analysis will enhance whole community collaboration around disaster risk reduction, identify indicators of community resilience and opportunities to introduce advanced technology solutions, empower communities with decision-support capabilities to enable pre-event risk planning and adaptive recovery in the post-event environment, and enable faster decision-making.

Community Resilience Testbeds

CHALLENGE: FEMA and state and local communities need access to new and emerging technologies and innovations to strengthen critical infrastructure, mitigate hazard vulnerabilities, and strengthen residential housing and commercial structures to reduce disaster risks, losses, and damages allowing communities to rebound more quickly.

IMPACTS: Providing the ability to evaluate and validate new solutions and make more informed technology investments toward keeping pace with evolving disaster risks will expand state and local capacity, reduce fatalities and property losses, and prioritize and optimize its pre- and post-disaster grant programs.

Next Generation Disaster Proofing

CHALLENGE: FEMA and state and local communities need access to new and emerging technologies and innovations that reduce risk, improve protective measures, optimize mitigation investments, and reduce damages, disruption, and costs of disasters.

IMPACTS: Providing innovative technology and tools to FEMA operations, pre- and post-disaster assistance programs, communities in the NFIP, and state and local partners and critical infrastructure operators will allow FEMA to keep pace with the evolving flood risk, enable state and local prevention and recovery capacity, and reduce fatalities and property losses.

Critical Infrastructure Resilience

CHALLENGE: Critical infrastructure owners and operators need data-driven information on position, navigation, and timing (PNT), electromagnetic pulse (EMP), and geomagnetic disturbance (GMD) threats and the impacts to their sectors, including up-to-date information on the actions they should consider for risk management and mitigation. PNT is an essential element for many critical infrastructures such as the electric grid, telecommunications, transportation, and emergency services. Other electronic capabilities within critical infrastructure ecosystems are susceptible to intentional attack or a natural occurrence of EMP and GMD.

IMPACTS: Providing best practices and tools to critical infrastructure owners and operators will allow them to understand, prepare for, and protect PNT capabilities and electronic systems against an EMP or GMD event. Enhancing the security and resilience of both government and private sector critical infrastructure will help safeguard the systems from disruption, corruption, and dysfunction by providing opportunities for innovative industry solutions to mitigating risks.

Countering Violent Extremism

Policy makers and operational end users need to make informed decisions to divert vulnerable individuals, prevent potential offenders, mitigate vulnerabilities, and enhance community resilience in the face of social and behavioral threats. Evidence-based research is needed to guide decisions that meet policy, operational, and public needs regarding improvements to public safety and violence prevention efforts implemented by federal, SLTT and non-governmental stakeholders.

Public Safety and Violence Prevention

CHALLENGE: DHS needs an analytical and qualitative approach to preventing, responding to, and recovering from acts of violence. One of the Department's top priorities is to protect citizens from terrorism and other homeland security threats; however, the drivers behind these acts are not fully understood. Targeted violence and terrorism represent a complex host of problems, crimes, and activities that are related to a number of threats.

IMPACTS: Advanced, evidence-based data collection and analysis will allow the HSE to enable education and awareness efforts to launch and reinforce a whole-of-society prevention architecture. The architecture would equip and empower local efforts from peers, teachers, community leaders, and law enforcement to minimize an evolving threat while emphasizing emergency preparedness and developing effective, situation-based responses. The program would increase understanding about approaches that work, fail, and are emerging in public safety and violence prevention efforts, while informing strategy, policy, and operations for DHS components and other key stakeholders.

First Responder Capabilities

Protecting and assisting first responders during any emergency involves providing the tools and equipment, current and accurate information, and efficient situation-specific procedures to aid first responders, emergency managers, and incident commanders as they respond to hazardous situations.

Personal Protective Equipment

CHALLENGE: DHS and related components need to determine priorities and methods for developing and distributing compact, effective personal protective equipment (PPE) that protects first responders from the health risks associated with exposure to biological, chemical, radiological, physical, electrical, or other hazardous elements in the operational environment.

IMPACTS: Available and viable PPE solutions along with adequate communication and training will help provide protection from serious injuries and illness associated with the exposure to hazards in the operational environment.

Explosives and Radiological and Nuclear Resilience

CHALLENGE: To safely and effectively respond to a bomb, radiological dispersal, or nuclear device detonation, first responders need improved training and equipment to prepare for and mitigate the consequences of such incidents. Response organizations require improvements in radiological-nuclear response management, incident characterization, initial response capabilities, medical care and triage, casualty and evacuee care, impacted-area stabilization and control, and site cleanup and decontamination.

IMPACTS: Providing improved response capabilities at the national and SLTT levels with increased agency preparedness, improved understanding of the impacts and risks, and technological solutions to radiological and nuclear capability gaps and mission needs will help protect responders while they work to control and mitigate damages as quickly and effectively as possible.

First Responder Technologies

CHALLENGE: Our nation's first responders need innovative technology to address high priority capability gaps to ensure the safe and effective performance of their duties. S&T must research the changing requirements for various situations, identify promising innovations, and evaluate potential investments in technology that will maximize the safe and effective execution of their duties. Needed solutions and technologies include data management and information sharing; gunshot detection, localization, alert, and recording; hands-free presence of life through walls detection, localization, alert, and recording; crowd control; and improvised explosive devices (IED) defeat.

IMPACTS: Providing responder organizations with effective and relevant technologies will strengthen the response community's ability to protect from and respond to disasters and save lives.

Public Safety Communications

CHALLENGE: DHS components need advanced mission-critical communications solutions. While the introduction of broadband networks has increased the ability to share data and provided an alternative voice network, it has resulted in a more complex environment requiring interoperability across networks. Although the evolution and diversity of emerging networks such as 5G, Smart Cities, Internet of Things, and advanced computing have provided advanced capabilities that can be leveraged by DHS components and first responders, they present challenges for ensuring reliable, interoperable, and secure communications. These challenges include the effective use of applications and services while addressing threats and challenges (spectrum, utilization, network resiliency, cyber, and physical attacks).

IMPACTS: Providing highly available and resilient critical communications and information sharing capabilities for DHS components and first responders using emerging technologies and communications networks will enable the efficient and effective use of networks and spectrum.

Bomb Defeat Operations Support

CHALLENGE: Bomb squads and SWAT teams need innovative tools to address emerging threats from active shooters, complex coordinated attacks, and IEDs. Bomb technicians need capabilities to preserve life and property once an IED has been discovered. Responders require an ongoing evaluation of needs, required capabilities, and potential investments in innovations to conduct their missions more safely, effectively, and efficiently.

IMPACTS: Advanced solutions to shooting and explosive threats will strengthen technicians' and responders' abilities to safely neutralize the highest priority threats and effectively counter terrorist and criminal activities while saving lives and protecting property.

Training and Performance Optimization

CHALLENGE: DHS components and law enforcement agencies need enhanced training infrastructure and research-based mission execution training capabilities that maximize proficiency, effectiveness, efficiency, safety, and more capably support the DHS mission to respond to local, national, and international disasters or emergencies. Training needs to deliver the skills and flexibility required for a variety of conditions including operating in uncertain, time-constrained, and hazardous environments.

IMPACTS: Providing HSE end users and first responders with improved training methods, technologies, and tools will result in operational performance increases and an increase in national security. More effective and efficient training measurably improves performance and is directly correlated to increased preparedness, safety, robustness, and capacity for rapid recovery and adaptability.

Physical Security

Ensuring safety requires effective screening for potential threats in unstructured crowds within soft-target venues and crowded spaces without impacting traffic and while maintaining privacy.

Soft Targets and Crowded Spaces

CHALLENGE: DHS needs to screen people and their belongings in soft targets and crowded spaces, such as surface transportation centers, without limiting traffic or invading privacy. The unique requirements of these environments include large, open systems with no fixed checkpoints, unstructured crowds, extremely high throughput, and an unalterable existing infrastructure within which screening technologies must fit.

IMPACTS: Effective technologies will provide a layered and integrated capability to safely screen people and their belongings for potential threat materials and contraband in unstructured crowds in soft-target venues and crowded spaces without impacting the speed of travel and while maintaining individual privacy.

Science and Technology