~~FOUO / For Official Use Only~~

Department of Homeland Security

Strategic Issue Paper Summaries

Presidential Transition 2016-2017

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.

(b)(5)

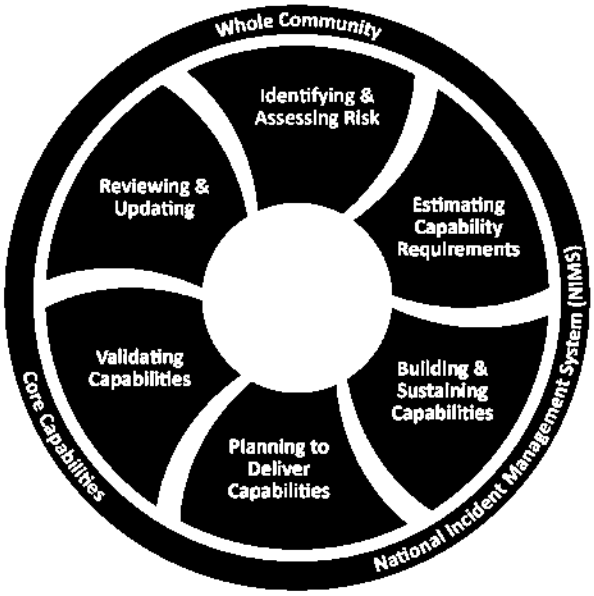
Return to Top

NATIONAL PREPAREDNESS SYSTEM

[2]CBP's Preclearance, operating at 15 locations worldwide, allows for advance inspection of passengers before they board U.S.-bound flights, while its range of international Trusted Traveler programs, provides pre-vetted and approved, low-risk travelers expedited clearance upon their arrival in the United States.

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.

- The National Preparedness System was established to strengthen the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation. The National Preparedness System is an integrated set of guidance, programs, and processes to enable the Nation to meet the National Preparedness Goal, which is: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."
- Nationwide, this translates into more disciplined and deliberate planning, organizing, equipping, training, and exercising among first responders, emergency managers, public health officials, and health care providers through their own investments as well as FEMA grants, which have totaled more than $47 billion since 2002.



- The scope and scale of the National Preparedness System is both large enough and detailed enough to prepare for and use during catastrophic incidents as well as those managed by a single local emergency services organization. Using an all-hazards and whole community approach, the System is adaptable to all threats that the Nation faces.
- Through the National Preparedness System, FEMA assists the whole community in establishing goals, objectives, and performance measures that enable communities to measure improvements in capabilities and statewide preparedness.
- Within the annual National Preparedness Report (NPR), FEMA identifies progress and challenges to address in building and sustaining the Nation's preparedness.
  - National areas for improvement include Cybersecurity, Economic Recovery, Housing, Infrastructure Systems, Natural and Cultural Resources, and Supply Chain Integrity and Security.
  - Three of these – (1) Cybersecurity, (2) Housing, and (3) Infrastructure Systems – have been identified as areas for improvement in the NPR for five consecutive years.
  - Capabilities that need to be sustained include Planning; Public Health, Healthcare, and Emergency Medical Services; and, Risk and Disaster Resilience Assessment.
- Maintaining and strengthening the National Preparedness System and building the capabilities of non-federal partners to reduce reliance on the Federal government, requires focused action in areas that include:

~~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.~~

- Continue the development and implementation of the National Qualification System in order to advance integrated mutual aid across the whole community.
- Develop the guidance, tools, and technical assistance necessary to aid communities in building, sustaining, and delivering capabilities.
- Advance an integrated National Training and Education System that ensures the personnel responsible for delivering capabilities are receiving the right training at the right time.

Return to Top

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.~~

EMERGING INFECTIOUS DISEASE THREATS

- History has shown that highly infectious diseases emerge or reemerge with some regular frequency and could greatly hamper DHS's ability to perform critical mission functions. The impacts of these incidents on the United States, even if initially identified overseas, are exacerbated by factors such as globalization, international trade, reduced international travel times/enhanced travel routes, increased density of human populations in urban centers, and human encroachment into animal habitats.
- In close coordination with the Department of Health and Human Services (HHS) and the Centers for Disease Control and Prevention (CDC), DHS strives to protect the American public from emerging infectious disease (EID) threats through multiple actions such as:
  - Early warning from the National Biosurveillance Integration Center (NBIC);
  - Helping to prevent these diseases from crossing our borders; and
  - Coordination of the inter-agency response providing support to state, local, tribal, and territorial (SLTT) governments.
- DHS is also focused on protecting our workforce from EID threats, and ensuring the Department can continue to perform its critical missions in the face of these threats.
- The following trends are impacting the EID issue area, and will require changes in operational posture, policy, and/or resource allocation:
  - The threat has evolved. Over the past few years, we have seen numerous infectious diseases emerge with potential impacts to the American public and the DHS workforce, including H1N1, Ebola, and Zika. These outbreaks have required unprecedented levels of cooperation across DHS components and with interagency stakeholders.
  - Technological advancements have enhanced the ability to identify EIDs of potential concern (when in the past, they may have had been attributed to other etiologies).
  - The complexities of inter-agency response have increased with new capabilities in and responsibilities of some Departments and Agencies.
  - Since its launch in 2014, the Global Health Security Agenda (GHSA) has focused U.S. and international attention on building countries' capacity to help create a world safe and secure from infectious disease threats. Inherent to GHSA are requirements for participating countries to elevate global health security as a national priority in an effort to contribute to global health.
  - Government Accountability Office (GAO) reviews have found that DHS programs for biological early warning must evolve to meet today's threats. Success will require increased cooperation from external stakeholders (including federal partners).

Return to Top

~~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.~~

CHEMICAL THREATS

- ~~(U//FOUO)~~ DHS assesses that ISIL is increasingly interested in conducting and inspiring more complex attacks against the West[3]. ISIL-linked adversaries may consider incorporating toxic materials into attacks in the West with the aspiration of increasing fear, enhancing attack lethality, and adding greater complexity to response efforts. DHS believes that ISIL-inspired homegrown violent extremist (HVEs), or other domestic actors, who choose to pursue attacks with toxic materials most likely would employ commercially available toxic industrial chemicals (TICs) and use crude dissemination methods such as explosive dispersal, contaminating surfaces, poisoning food or water, or releasing gasses from pressurized tanks or via improvised chemical devices.
- When responding to a chemical attack, time matters for saving lives and managing resources. The window of opportunity to positively impact the response occurs in the first 2-4 hours. Most Federal resources are not available to support the immediate state and local response during that time. Therefore, the greatest Federal government impact to save lives must be made long before the incident occurs.
- Courses of action:
  - Work with chemical industry and the private sector to secure toxic chemicals in the supply chain.
  - Expand programs to train state and local first responders and leadership.
  - Maintain border and transportation security to stop bad actors before they have a chance to deploy chemicals as weapons.
  - Provide threat information and guidance to the state and local response community to enable a timely response and efficient decision making in the event of a chemical release.

Return to Top

[3] ~~(U//FOUO)~~ For more information please see DHS-FBI-Delaware Information Analysis Center-Ohio Strategic Analysis &Information Center Joint *Intelligence Assessment* "(U//FOUO) Toxic Materials Unlikely but Possible Weapon Choice for ISIL- Inspired or Directed Homeland Attacks" dated 23 May 2016

~~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.~~

BIOLOGICAL THREATS

- The nation faces risks from biological attacks or accidental releases of pathogens with the potential to produce destabilizing effects and greatly impact Department of Homeland Security (DHS) operations and the American public.
- The United States and its allies face ongoing and ever evolving threats from violent extremist groups or individuals inspired by these groups. The global reach of groups like Islamic State (IS) and the widespread availability of biological materials and expertise increase the risk of a terrorist attack using a biological Weapon of Mass Destruction (WMD).
- DHS's goal is to prepare our communities and our workforce to prevent, detect, mitigate, respond to, and recover from biological incidents quickly in order to save lives and minimize wide-spread or cascading impacts.
- The following trends are impacting the biological threats issue area, and will require changes in operational posture, policy, and/or resource allocation:
  - The threat continues to evolve. The biological weapons threat has expanded from large State-sponsored programs to include global terrorist groups and lone wolf violent extremists.
  - Government Accountability Office (GAO) reviews have found that programs for biological early warning must evolve to meet today's threats and provide the advanced warning needed to save lives. To achieve these ends the Department must foster increased cooperation across multiple partners and stakeholders, both within and outside the Department—to include various Federal partners.

Return to Top

~~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.~~

ENHANCING INTERNATIONAL AVIATION SECURITY

- Numerous attempted attacks and evolving, complex threat streams over the past decade clearly demonstrate terrorists' pervasive focus on targeting the aviation sector.
- A key mechanism for countering these threats is an informed, comprehensive application of security measures tailored to the threat and applied at those airports and air carriers most likely to be directly or indirectly affected.
- International inbound aviation represents the largest share of total aviation security risk (89%) for which the Transportation Security Administration (TSA) is primarily responsible.
- As such, TSA works closely with our U.S. Department of Homeland Security (DHS) partners, as well as foreign governments and industry stakeholders, to mitigate the risk on inbound international flights entering the United States TSA also works closely with foreign governments to negotiate agreements to allow the carriage of Federal Air Marshals to and from Last Point of Departure airports.
- Since 2014, the total terrorist plots/attacks directed toward the West and Europe have increased over 73%.
- Recent aviation security incidents such as the terrorist attacks in Paris (November 2015) and Brussels (March 2016), the crashes of Metrojet 9268 in the Sinai Peninsula (October 2015) and Daallo Flight 159 in Somalia (February 2016), and the attack on the Istanbul Airport (June 2016) illustrate the need for consistent leadership engagement on international aviation security.
- The 114th Congress has provided a considerable amount of oversight on aviation security, passing legislation granting TSA new authorities for international engagement and requesting reports and oversight of international activities via the Federal Aviation Administration (FAA) Extension, Safety, and Security Act of 2016 (P.L. 114-190), which became law in July 2016.
- Per congressional request, the Government Accountability Office began in August 2016 an audit of TSA's foreign airport assessments and air carrier inspections; the completion date is to be determined.

Return to Top

~~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.~~

COMBATING TRANSNATIONAL CRIMINAL ORGANIZATIONS

- In 2011, the *National Strategy to Combat Transnational Organized Crime* was signed and stated in part "Criminal networks are not only expanding their operations, but they are also diversifying their activities, resulting in a convergence of transnational threats that has evolved to become more complex, volatile, and destabilizing. These networks also threaten U.S. interests by forging alliances with corrupt elements of national governments and using the power and influence of those elements to further their criminal activities."

- Transnational criminal organizations (TCO) rely on revenues generated through the sale of illegal drugs, counterfeit goods, human trafficking and smuggling, and other criminal activities. These organizations, whether structured or decentralized in nature, continue to capitalize on technological innovation, including new platforms to sell illicit goods, innovative ways of moving money, tools for coordinating operations, and a variety of other criminal and cyber activities.

- Disrupting these complex illicit networks requires that DHS contribute to a well-informed and agile U.S. government and global response. Through integration of capabilities, DHS provides actionable, tactical and strategic intelligence and information across its operational component organizations. This not only enables unique DHS interdiction and investigative capabilities, but also those of domestic and foreign partners.

Return to Top

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.

REAL ID

- REAL ID[4] is a coordinated effort by the states[5] and the Federal Government to improve the reliability and accuracy of state-issued driver's licenses and identification cards (ID) in order to prevent the fraudulent issuance or use of these documents and, thereby, inhibit terrorists' ability to evade detection.
  - The REAL ID Act of 2005 ("the Act") (P.L. 109-13): 1) sets minimum requirements for the secure issuance and production of state-issued driver's licenses and IDs; and 2) prohibits Federal agencies from accepting driver's licenses and IDs issued by noncompliant states for official purposes (i.e., entering nuclear power plants, accessing Federal facilities including military installations, and boarding federally-regulated commercial aircraft).
  - It does not authorize DHS to: regulate states (state participation is voluntary); create a national ID; or create a Federal database of driver information.
- DHS has expended considerable effort to advance implementation of REAL ID through coordination with Governors, and their representatives, Department of Motor Vehicle Administrators, state legislators and national state associations.
- There are some states that have taken a "wait and see" stance to see if DHS is truly serious about REAL ID implementation and as a result, DHS has established strict enforcement dates.
- In 2017, DHS will: 1) determine whether states are compliant; 2) grant extensions to individual noncompliant states as appropriate;[6] and 3) prepare the public for enforcement related to boarding commercial aircraft.[7]
- The statutory requirements of the Act are the main driver for DHS enforcement.[8]
  - 13 states and 1 territory are not yet committed to becoming compliant (see Table 1 and Fig. 1) and could be affected when the Transportation Security Administration (TSA) begins enforcement on January 22, 2018. At that time, TSA will no longer accept licenses issued by noncompliant states (without extensions) for boarding commercial aircraft or entering an airport's sterile area.
- Potential courses of action include: adhering to the current enforcement plan; seeking statutory and regulatory changes to reduce compliance costs for states; or adjusting the enforcement schedule, which may necessitate regulatory changes.

---

[4] Not an acronym.

[5] "State" is defined as the 50 states; the District of Columbia; and the territories of American Samoa, Commonwealth of Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands.

[6] Section 205(b) of the Act authorizes the Secretary of Homeland Security to grant states with an extension of time to meet the REAL ID requirements if the state provides adequate justification for noncompliance. Federal agencies may continue to accept driver's licenses and IDs issued by noncompliant states with an active extension.

[7] *Statement by Secretary Jeh C. Johnsan an The Finol Phase af REAL ID Act Implementation*. January 8, 2016. https://www.dhs.gov/news/2016/01/08/statement secretary jeh c johnson final phase real id act implementation#

[8] Under a 2012 interagency plan, the Federal Government has been phasing in REAL ID, an approach that has encouraged states to make progress by providing clear, realistic consequences for continued noncompliance.

Return to Top

~~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 BIG DATA

The Department of Homeland Security (DHS) is working to make its data a strategic asset for the homeland security enterprise to better inform operations, business processes, and decision-making. The DHS Data Strategy will provide a foundation of enterprise data management values, guidelines, and principles to leverage its data assets to create 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 response and protection. 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 Science & Technology Directorate's (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 Data Analytics Engine 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 Office of the Chief Information Officer (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.
Standards and Enforcement	DHS shall define and enforce standards for enterprise data management.
Compliance	The Department must ensure that it complies with all legal and policy requirements in the maintenance collection, use, and dissemination of its data.
R&D	S&T leads the Department's efforts to innovate and evaluate emerging big

~~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.~~

	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.

Return to Top

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.

PREVENTING NUCLEAR TERRORISM

- The grave threat of nuclear terrorism against our nation has been stressed by the current U.S. president and his predecessor. A terrorist nuclear attack could involve one or more nuclear devices, each with an explosive yield sufficient to cause massive casualties and devastation to a metropolitan area, damaging the nation's sense of security and resulting in major worldwide disruptions to commerce, trade, and travel.[9]
- Because of the catastrophic consequences, the Department must continue to prioritize prevention of nuclear terrorism. Bolstering capabilities at the federal, state, local, territorial, and tribal levels helps defend the nation. Working with the international community helps to enhance nuclear security worldwide, well beyond our borders.
- But maintaining an appropriate sense of urgency towards low-probability, high-consequence threats such as nuclear terrorism is challenging. Other, more likely threats may demand more immediate attention. Ensuring that the homeland security enterprise is engaged in preventing a potentially catastrophic terrorist nuclear attack is critical.

Return to Top

[9] Alternatively, a "dirty bomb," dispersing radioactive material using conventional explosives, could deny access to a portion of a city for some time but cause significantly fewer deaths.

~~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.~~

ARCTIC / POLAR

- Access to Arctic sea routes is increasing due to climate change and improved vessel capabilities (e.g. Polar Code compliant vessels).
- Diminishing Arctic sea ice may provide shippers a substantially shorter route between Asia and Europe, and opens larger areas to natural resource exploration/exploitation not only at sea but also within United States Arctic terrestrial domain (e.g., rare earth metals in northern Alaska).
- Increased global access to the Arctic may present challenges to U.S. sovereignty, especially in areas where there are competing claims to the Outer Continental Shelf, exacerbated by the U.S. not being a signatory to the United Nations Convention on the Law of the Sea.
- Conflicting territorial claims in the Arctic may present challenge to U.S. position on freedom of the seas and navigation, including disputes with Canada.

Importance

- The U.S. is an Arctic nation and must maintain the ability to protect U.S. borders, exert our sovereignty over our territorial seas and Exclusive Economic Zone, and ensure the safe, secure and environmentally-responsible maritime activity in U.S. Arctic waters.

Trends

- Trend 1: The Arctic is warming at a faster pace than the rest of the world – nearly twice the global rate over the last 100 years which has lead to diminishing sea ice and increased access to Arctic sea routes. The pace of warming has accelerated markedly in the past three decades.
- Trend 2: Increased maritime activity, including commercial shipping (passenger and cargo), energy exploration and exploitation, and recreational vessels will use Arctic sea routes in or adjacent to U.S. waters.
- Trend 3: Increasing maritime activity funnels through "choke points" such as the Bering Sea, significantly elevating risks within traditional Coast Guard missions (e.g., Search and Rescue, or SAR).
- Trend 4: Arctic and non-Arctic nations and states have increased their focus on producing polar-capable vessels and icebreakers to enable shipping through Arctic sea routes, providing both partners and competitors with greater Arctic access than that of the U.S.

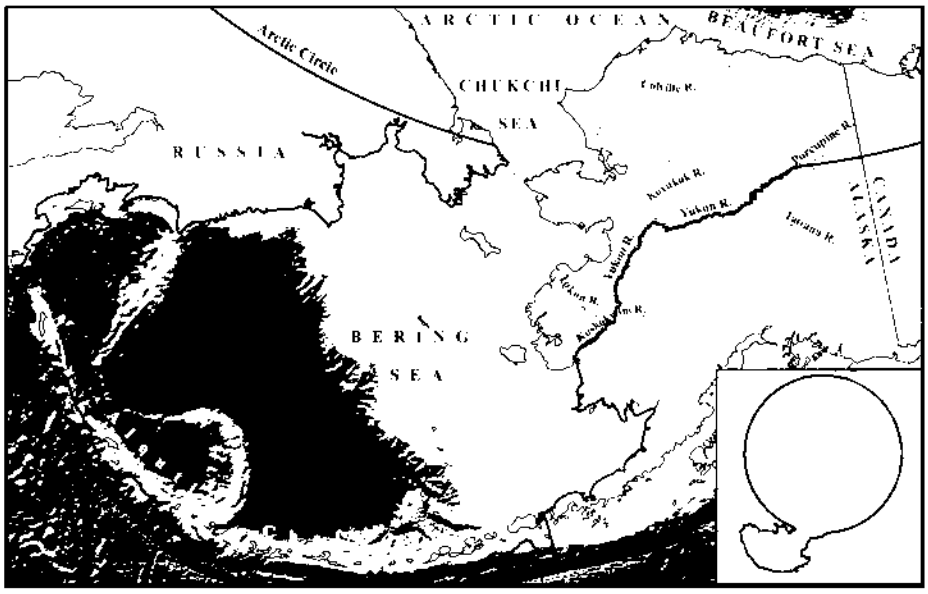
Major Risks

- Increased human activity in the Arctic presents risks to the integrity of U.S. borders and environmental and maritime safety risks associated with trans-Arctic shipping and mineral exploration/exploitation.
- The remote and harsh nature of the Arctic and lack of infrastructure (including ports, navigational aids, reliable hydrographic data, and communications) and the lack of consistent adequate domain awareness creates a difficult incident management posture.

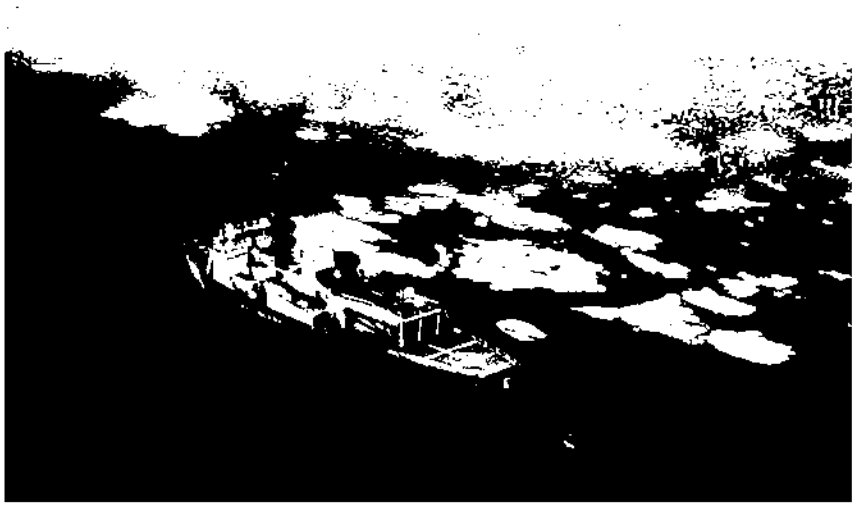
~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency intra-agency material. You are hereby notified that any dissemination, 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.~~

Courses of Action

- Course of Action 1: Maintain year-round Polar access via icebreakers and air capabilities.
- Course of Action 2: Build robust partnerships with states and groups with Arctic equities and expertise.
- Course of Action 3: Work cooperatively to protect the Arctic's rich marine environment.



Arctic Boundary as defined by the Arctic Research and Policy Act (ARPA) of 1984, Public Law 98-373, at 15 USC §4111.



The Coast Guard Cutter Polar Star, the nation's only heavy polar icebreaker, cruises on the ice edge of the Chukchi Sea north of Wainwright, Alaska, in July 2013. (PETTY OFFICER 1st CLASS Sara Mooers / U.S. Coast Guard)
Source Publication: http: www.adn.com opinions 2016 08 15 u-s-needs-more-icebreakers-to-keep-watch-in-arctic

Return to Top

~~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.~~

INFORMATION SHARING WITH FOREIGN PARTNERS

- The DHS Office of Policy (PLCY) coordinates all DHS engagement with foreign governments and international organizations. PLCY works closely with the DHS Components, as the operators that implement any international information sharing arrangements, to ensure agreements and arrangements are in support of and alignment with Departmental international engagement priorities.
- DHS works closely with the Departments of State and Justice, where applicable, when negotiating new arrangements that may impact the U.S. government.
- DHS regularly shares information with U.S. government intra-agency partners and key foreign partners to aid in the identification of criminals, terrorists and illegal immigrants before they can target the United States or our allies for nefarious purposes.
- Data shared may be derogatory in nature (e.g. criminal histories, immigration violations, or terrorist watchlists), transactional (e.g. travel history) or identity (e.g., names).
- International information sharing activities are influenced by legal, operational and policy frameworks, and the nimble threat environment. Such factors may include, but are not limited to:
  - The Visa Waiver Program (VWP) requirements;
  - Global migration trends, including from Central America to the U.S. and from the Middle East to Europe;
  - Exploitation of global travel systems by foreign fighters;
  - Mandate to identify, dismantle, and/or disrupt Transnational Crime;
  - The potential for criminals and terrorists to circumvent some U.S. screening programs by obtaining new identities and travel documents in third countries;
  - U.S. legislation that prohibits the use of criminal history for immigration or non-law enforcement purposes;
  - International debates over privacy particularly within the European Union.

Return to Top

~~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.~~

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
Counterterrorism

OVERVIEW

- Counterterrorism (CT) is the primary mission of the U.S. Department of Homeland Security (DHS) and a principal reason DHS was founded after the 9/11 terrorist attacks. The CT mission requires a "whole-of-government" approach to ensure effective coordination across the Department, as well as with interagency and international partners.
- Almost all DHS Components and headquarters elements participate in the Department's CT mission. The operational Components carry out most of DHS's CT activities (see Appendix A for descriptions of Component CT activities), with DHS headquarters providing coordination and policy direction.
- The principal counterterrorism official within the senior leadership of DHS is the DHS Counterterrorism Coordinator (CT Coordinator), who is designated by, and receives a Delegation of Authority from, the Secretary. The CT Coordinator ensures DHS' CT efforts are appropriately developed, coordinated, and implemented. A decision on this designation will need to be made early in the transition process.
  - The DHS CT Coordinator does not have directly assigned staff. There are currently roughly a dozen career CT staff members, detailed from six Components, who assist the DHS CT Coordinator in carrying out duties delegated by the Secretary.
- The DHS Counterterrorism Advisory Board (CTAB) is the senior intra-DHS body of senior leaders from DHS components and offices that carry out CT-related operational, information sharing, and policy related activities. The CTAB charter has a Chair (the DHS CT Coordinator) and two Vice Chairs (the Assistant Secretary for Policy and the Under Secretary of Intelligence and Analysis). In practice, for the past two years, the Secretary or Deputy Secretary has chaired the weekly meetings of the CTAB. A decision whether to keep or modify this structure will need to be made in the transition process.
- The terrorism threat is evolving and remains significant as terrorist attack planning and operations become more decentralized. Terrorist groups continue to demonstrate their reach and relevance through their ability to export violence from safe havens in the Middle East to the West by exploiting porous borders and through a robust online recruitment and incitement campaign.
  - Trend 1 - Terrorists continue to threaten aviation security, both internationally and domestically, through attacks at airports, airport personnel insider threats, and attempts by terrorist groups to conceal and place explosive devices on aircraft via air cargo, passenger carry-on, and checked baggage.
  - Trend 2 - The Homegrown Violent Extremist (HVE) threat arises from individual or small group efforts directed, enabled, or inspired by terrorist groups, generally through the use of social media platforms. HVEs often use simple tactics such as small arms and improvised explosives. There has been a continued increase in HVE plots and attacks both in the United States and abroad.

~~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.~~

- Trend 3 - Internationally, groups like the Islamic State of Iraq and the Levant, al-Qa'ida, Lebanese Hizballah, and others operate in terrorist safe havens, plot attacks, and use a variety of media to inspire others to carry out violent actions in the United States, Europe, South Asia, and elsewhere. Overall, these have also increased in recent years.
- Trend 4 – Terrorists are increasing their focus on attacking civilian "soft" targets, as critical infrastructure, government, and military targets are further "hardened."

DETAILED DISCUSSION

Role of DHS in CT

- Section 101(b)(1) of the Homeland Security Act begins "The primary mission of the Department is to—(A) prevent terrorist attacks within the United States; (B) reduce the vulnerability of the United States to terrorism; (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States...."
- In addition to DHS's CT operational activities at the border, domestically, internationally, and in cyberspace, DHS participates in CT decisions by the President and the National Security Council on most national security issues.

Issue Background

- The U.S. Government uses military, intelligence, and border security tools to protect the Homeland. Border security and enforcement continues to be an essential part of protecting the United States.
- Many of DHS's lines of effort contribute to protecting the United States from terrorist attacks. Additionally, effective coordination of DHS CT-related capabilities, and coordination of DHS activities with other programs and policies is essential to success in the counterterrorism mission.
- DHS prepares federal, state, local and private sector partners for coordinated, complex attacks; to impede the use of explosive precursors; enhance the security of soft targets; and counter violent extremism in our communities.
- DHS hosts engagements following a national security incident of significance with impacted communities, as well as faith-based groups, non-governmental organizations, academia, and local leaders through community engagement events (such as roundtables, community awareness briefings, youth engagements, and incident communication coordination calls.)
- Our international allies' border and immigration security efforts are sometimes vital to our homeland security efforts. DHS works to understand disparities in how border, aviation, and maritime security is handled among different countries, and the impact of those security postures on U.S. security. DHS works to enhance the capabilities of counterparts, recognizing that this is often the most effective means to keep foreign terrorists from threatening the United States.
- In recent years, DHS has increased the number of agreements or arrangements to share terrorism related data, stationed CBP officers and ICE/HSI agents overseas to work with counterparts, and enhanced programs like Preclearance and the Visa Waiver Program with

~~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.~~

counterterrorism security measures. As a result, the identities of thousands of known or suspected terrorists have been shared and used to vet travelers and identify threats.

Courses of Action

- DHS should continue programs that are effective at detecting and disrupting terrorist threats to the United States. Those programs need to be effective every day.
- DHS should intercept and address potential threats at the earliest possible opportunity, which many times is overseas, before such threats reach the United States.
- The U.S. Government, through DHS, should continue to integrate border and immigration security tools and information systems with information from the Intelligence Community, the U.S. military, and U.S. embassies overseas.
- DHS should continue to share with international partners information on terrorists and related travel data, criminals, and derogatory immigration-related data.
- DHS should increase engagement with the Departments of State and Defense for greater collaboration in homeland security related foreign assistance to help international partners build capacity to combat terror.
- The new DHS Secretary will need to designate the DHS CT Coordinator. It is essential that the CT Coordinator is positioned to coordinate effectively across DHS and represent DHS in the interagency at the Deputies level, as well as with international counterparts.
- The Secretary will also need to determine if the CT staff should be permanently assigned to the CT Coordinator.
- By Charter, the DHS CT Coordinator chairs the DHS Counterterrorism Advisory Board (CTAB), which coordinates Department-wide CT issues, including the management of the National Terrorism Advisory System. Currently, the Secretary or Deputy Secretary to chair the CTAB. The membership is comprised of all the DHS Components, the Office of General Counsel, Office of Policy, and Office of Public Affairs. The Offices of Civil Rights and Civil Liberites and Privacy also attend. A decision on whether to replicate or modify this structure will need to be made early in the transition process.
  - The CT Coordinator Staff assists the CT Coordinator with executing the CT Coordinator's delegated authorities; manages CTAB meetings; and represents the Department at the National Security Council's CT Security Group (CSG) and various other Interagency Policy Committees of CT relevance to DHS. CT Coordinator Staff also provides expert CT policy advice to the Secretary and senior DHS staff.

Key Partnerships

- DHS works closely with international counterparts – including Europe, the Middle East, and North Africa – to leverage each other's capabilities to thwart terrorist threats and to coordinate enforcement actions.
- DHS federal interagency partners on CT include the FBI, through Joint Terrorism Task Forces; the Departments of Defense, Justice, and State; and the Intelligence Community. DHS often uses funding from the Departments of State or Defense to provide homeland

~~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.~~

security-related foreign assistance to help international partners build capacity to combat terror.

- Ongoing engagement occurs with state, local, tribal, and territorial law enforcement, state homeland security officials, and first responders. First responders are likely to provide immediate response to terrorist attacks.
- Ongoing engagement also occurs with the private sector, including industry owners and operators and security professionals from the critical infrastructure sectors.

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.

Appendix A: Descriptions of Component Counterterrorism (CT) Activitites

U.S. Citizenship and Immigration Services (USCIS)*	USCIS oversees lawful immigration to the United States, including adjudication of immigration and citizenship applications. In carrying out its duties, USCIS ensures that immigration benefits are not granted to individuals who pose a threat to national security or public safety, or who seek to defraud our immigration system, detects and combats immigration benefit fraud in the application process, and removes systematic and other vulnerabilities in order to enhance the integrity of the legal immigration system.
U.S. Coast Guard*	The Coast Guard employs a layered, defense-in-depth strategy designed to detect, prevent, and defeat terrorism threats as far from our shores as possible. Coast Guard counterterrorism activities rely heavily on robust intelligence and maritime domain awareness programs, and include domestic and international regulatory regimes aimed at securing our nation's ports and waterways, and the Maritime Transportation System. The Coast Guard also possesses highly specialized tactical law enforcement and maritime security teams that can deploy far offshore to neutralize known threats.
U.S. Customs and Border Protection (CBP)*	CBP focuses on the identification of high-risk individuals and cargo entering the United States at and between the ports of entry to intercept threats at the earliest possible moment. This includes positioning of U.S. law enforcement professionals overseas, employing sophisticated targeting systems to detect risk, capacity building through engagement with international partners and information sharing with our law enforcement and intelligence community partners. CBP works to provide actionable, tactical and strategic CT intelligence to CBP officers, agents, and our operational partners.
Office of Community Partnerships (OPC)	OCP's objective as the Department's leader in countering violent extremism (CVE) is to support, improve, expand and coordinate the Department's existing community based CVE efforts by working with key stakeholders and partners at local, state, tribal, territorial, and federal levels. OCP's mission is to develop and implement a full-range of partnerships to support and enhance efforts by key stakeholders to prevent radicalization and recruitment to violence by terrorist organizations.

~~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.~~

Federal Emergency Management Agency (FEMA)*	The FEMA Administrator serves as the principal advisor to the President, National Security Council, and the Secretary on all matters relating to emergency management in the United States, and coordinates the federal response to credible and imminent terrorist threats or actual incidents, including conducting pre-incident consequence management planning in coordination with counterterrorism focused law enforcement operations. FEMA administers two state, local, tribal, and territorial preparedness programs that directly address the complex attack threat with emphasis on the Whole Community Response: the Joint Counterterrorism Awareness Workshop Series, and the Integrated Emergency Management Course. Since 2011, these programs combined have trained over 8,200 responders across 36 jurisdictions. As a direct result of these programs, specialized training in warm zone operations and Tactical Emergency Casualty Care has been provided to an additional 10,000 first responders.
U.S. Immigration and Customs Enforcement (ICE)*	ICE criminal investigators and immigration officers directly support counterterrorism investigations as participants in the FBI's Joint Terrorism Task Forces (JTTFs). ICE contributes its unique immigration and trade-based enforcement authorities as disruption options. ICE also conducts counter-proliferation investigations and investigates transnational criminal activity that supports terrorist movement via human smuggling pathways, and terrorist networks and support structures. This includes the ICE Visa Security Program, which identifies terrorists, criminals and other aliens ineligible for a visa. Domestically, ICE targets overstays and foreign student visa violators who exhibit specific risk factors, based on intelligence reporting and in-depth criminal research and analysis of dynamic social networks, to identify those who may pose a threat to national security or public safety. ICE's immigration enforcement arm identifies, arrests, and removes aliens who present a danger to national security or public safety, and those who enter the country illegally or otherwise undermine the integrity of U.S. immigration laws and border control efforts.
Office of Intelligence and Analysis (I&A)*	Pursuant to the Homeland Security Act of 2002, as amended, I&A provides personnel, intelligence support, technology, and training to state and major urban area fusion centers to support two-way information sharing between the federal government

~~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.~~

	and our state, local, tribal, territorial, and private sector partners. Fusion centers are uniquely situated to enhance the national threat picture and enable local officials to better protect their communities from a variety of threats. I&A collects information of intelligence value and produces unique insights on a full range of threats to the Homeland, including: terrorist targets, weapons, and tactics; terrorist identities and networks; violent extremists' radicalization and messaging; terrorist travel and facilitation; and U.S. immigration and aviation security for the full spectrum of homeland security stakeholders through timely and accurate published intelligence reporting, products, briefings, and direct engagement. I&A is one of the co-chairs of the CTAB.
National Preparedness and Protection Directorate (NPPD)*	NPPD helps protect federal and non-federal partners against cyber threat actors, including terrorist groups. NPPD also coordinates efforts to protect critical infrastructure from terrorism. NPPD regulates high-risk chemical facilities for security against terrorism and serves as the Department's lead for the Counter Improvised Explosive Device-mission. NPPD provides outreach and training to educate Commercial Facilities Sector partners, stakeholders, and the general public on suspicious behavior, protective measures, and risk mitigation. Broad programs include the "Hometown Security" campaign and the Active Shooter Preparedness Program. NPPD's Federal Protective Service (FPS) protects federal facilities and personnel who work or visit within. FPS employs risk-based deployments of law enforcement officers to mitigate threats and investigates threats directed at government employees and visitors to government owned and leased facilities. NPPD's Office of Biometric Identity Management (OBIM) helps to identify potential terrorist threats by matching, storing, sharing, and analyzing approximately 300,000 daily biometric queries against its database of more than 200 million identities, serving customers across DHS, at other agencies including the Terrorist Screening Center, and other mission partners. OBIM also works with the National Counterterrorism Center to enhance terrorist records with

~~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 collected biometrics.
Office of Operations Coordination (OPS)*	OPS supports the Secretary, Components, the CT Coordinator, and the Counterterrorism Advisory Board (CTAB) prior to or during a response to a CT incident. OPS provides operations coordination, information sharing, situational awareness, the common operating picture, and Department continuity, enabling execution of the Secretary's responsibilities across the homeland security enterprise. This includes senior leader notifications, conferencing, executive communications, integrated national-level reporting, and decision support products. OPS oversees the National Operations Center (NOC), the DHS Crisis Action Process, the Secretary's Situation Room, and distributes the National Terrorism Advisory System Bulletins. OPS may activate the DHS Crisis Action Team to augment the NOC in support of the Secretary, the CT Coordinator or the CTAB.
Office of Partnership and Engagement (OPE)	OPE manages the "If You See Something, Say Something™" public awareness campaign, which is focused on raising public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law enforcement. The campaign has had a clear effect on societal behavior as there have been multiple instances where tips from the public have assisted law enforcement investigations, as seen with the bar owner who reported seeing the main suspect in the September 2016 New York/New Jersey attacks.
U.S. Secret Service (USSS)*	USSS engages in a multi-faceted approach to support USSS protective operations, including through the analysis of intelligence, investigation of threats, assessment of risk, and dissemination of intelligence information, specific to counter terrorism efforts and otherwise. USSS also provides briefings regarding terrorist trends and tactics to USSS protective divisions, headquarters representatives, and field offices; local, state, and federal law enforcement officials; and the U.S. armed forces. Additionally, pursuant to Section 105 of the USA Patriot Act of 2001, USSS's nationwide network of electronic crimes task forces are designed to prevent, detect, and investigate various forms of cyber crimes, to include potential terrorist attacks against critical infrastructure and financial payment systems.
Transportation Security Administration (TSA)*	TSA protects the U.S. transportation systems and the traveling

~~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.~~

	public by assessing intelligence related to transportation security and applying risk-based countermeasures such as: operational mitigation plans; Federal Air Marshals; passenger screening; compliance inspections and assessments at last-point-of-departure airports; information sharing with interagency partners and industry stakeholders; and deployment of Visible Intermodal Prevention and Response teams.

* CT Advisory Board voting members (the Office of Policy, a part of DHS Headquarters, is also a voting member and a co-chair of the CTAB, but is not listed above).

~~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
Enhancing International Aviation Security

OVERVIEW

- Numerous attempted attacks and evolving, complex threat streams over the past decade clearly demonstrate terrorists' pervasive focus on targeting the aviation sector.
- A key mechanism for countering these threats is an informed, comprehensive application of security measures tailored to the threat and applied at those airports and air carriers most likely to be directly or indirectly affected.
- International inbound aviation represents the largest share of total aviation security risk (89%) for which the Transportation Security Administration (TSA) is primarily responsible. The other 11% is comprised of domestic aviation and mass transit modes.
- As such, TSA works closely with our U.S. Department of Homeland Security (DHS) partners, as well as foreign governments and industry stakeholders, to mitigate the risk on inbound international flights entering the United States. TSA also works closely with foreign governments to negotiate agreements to allow the carriage of Federal Air Marshals to and from Last Point of Departure airports.
- Since 2014, the total terrorist plots/attacks directed toward the West and Europe have increased over 73%.
- Recent aviation security incidents such as the terrorist attacks in Paris (November 2015) and Brussels (March 2016), the crashes of Metrojet 9268 in the Sinai Peninsula (October 2015) and Daallo Flight 159 in Somalia (February 2016), and the attack on the Istanbul Airport (June 2016) illustrate the need for consistent leadership engagement on international aviation security.
- The 114th Congress has provided a considerable amount of oversight on aviation security, passing legislation granting TSA new authorities for international engagement and requesting reports and oversight of international activities via the Federal Aviation Administration (FAA) Extension, Safety, and Security Act of 2016 (P.L. 114-190), which became law in July 2016.
- Per congressional request, the Government Accountability Office began in August 2016 an audit of TSA's foreign airport assessments and air carrier inspections; the completion date is to be determined.

DETAILED DISCUSSION

- Through the DHS/TSA Foreign Airport Assessment Program, TSA identifies vulnerabilities at foreign locations, primarily through reviews of national programs, assessments of foreign airports to International Civil Aviation Organization standards, and inspections of air carriers that fly from those airports, as well as foreign repair stations. In addition, TSA conducts MANPADS vulnerability assessments at certain foreign locations.
- TSA works closely with the DHS Office of Intelligence and Analysis to assess threat information and formulate any necessary mitigation measures through Security Directives (SDs) and Emergency Amendments (EAs).
  - For instance, TSA may use SDs and EAs to require air carriers to apply additional screening measures to passengers based on the threat(s).

~~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.~~

- TSA also works closely with U.S. Customs and Border Protection (CBP) through its Preclearance program, operational in 15 foreign locations. The Preclearance program effectuates the screening of passengers at certain "last point of departure" (LPD) airports overseas according to standards commensurate to those in the United States. This process allows passengers to continue any connecting domestic travel without being rescreened. TSA is responsible for ensuring aviation security is commensurate with U.S. standards.
- TSA partners with DHS Science and Technology Directorate (S&T) as well as industry and international stakeholders to evaluate new and emerging technologies and other threat mitigation capabilities to assess efficacy of aviation security countermeasures.
- Additionally, TSA and CBP coordinate on advanced passenger data and other information for the vetting of passengers arriving from overseas, which TSA checks against the Terrorist Screening Database (TSDB) through its Secure Flight vetting system.

Issue Background

- TSA is required by law to assess foreign airports with LPD service to the United States and to inspect foreign air carriers that fly into the United States, as well as U.S. aircraft operators. There are approximately 280 LPD airports in approximately 100 countries (this varies due to seasonal service changes and carrier decisions to start/terminate service).
- In FY15, TSA accomplished the following:
  - 289 Air Carrier Inspection Visits
  - 146 Foreign Airport Assessments
- TSA uses the Foreign Airport Assessment Program to identify existing and potential vulnerabilities at the specified airports and leverages a risk-based methodology to determine if an airport should be assessed on a 1-, 2-, or 3-year cycle. TSA conducts more frequent visits at higher-risk locations.
- TSA conducts air carrier inspections, both domestic and foreign, for LPD flights to the United States. Inspections are conducted on an annual or semi-annual schedule based on identified vulnerabilities. Inspections are also conducted on all domestic air carriers that have flights in any foreign location, regardless of whether the operation is at an LPD airport.
- All foreign air carriers and U.S aircraft operators flying to/within/over the United States are required to submit their Master Crew Lists to TSA for vetting against the TSDB. In addition, all air carrier/aircraft operator personnel working at U.S. stations (airports) are vetted when they receive their Security Identification Display Area (SIDA) badge. When directed by TSA, air carriers and aircraft operators must remove any crewmember from their Master Crew List.
- TSA continuously evaluates intelligence to prepare for new and emerging threats while working internationally with host governments, aviation authorities, and industry stakeholders to mitigate vulnerabilities at high-risk airports and to raise security standards above those required by the International Civil Aviation Organization (ICAO)

Courses of Action

- Additional legislative authorities via the FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) enables TSA to donate security screening equipment to locations overseas, addressing a previous gap that permitted TSA to only loan or lease equipment, or to work through a third party for donation of excess property. This new

~~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.~~

authority will allow TSA to help elevate security screening at locations overseas, better addressing the inbound international threat.

- TSA also received statutory authority for international training and capacity development. This authority allows TSA to expand current international training and course offerings to consider additional avenues for increasing capabilities in screening operations, airport security, and risk management at LPD airports to the United States. In addition, TSA also invites select foreign government aviation security personnel to participate in some of its training programs, such as Federal Air Marshal Service training.

- TSA is working on several key projects to continue enhancing global security standards:
  - TSA has undertaken a proposal to work with a foreign government's aviation authority and other key personnel to provide on-the-ground mentoring between transportation security specialists and airport stakeholders to address consistently poor findings during TSA airport assessments.
  - TSA is also engaging in development of regional strategic plans, creating specific tailored options for key ICAO Member States in different areas of the world to assist them in becoming regional leaders in aviation security.
  - Over the past year, TSA has offered training, guidance, and resources to aid its foreign partners in addressing insider threat risk-related vulnerabilities and implementing robust quality control programs.

Key Partnerships

- TSA collaborates closely with all its foreign partners through its network of 29 Transportation Security Administration Representatives (TSARs), International Industry Representatives (IIRs), TSA inspectors, and Headquarters personnel to identify and mitigate threats to aviation security.
- When incidents occur, such as the Brussels attack or the downing of the Metrojet aircraft, TSARs and IIRs coordinate with the Department of State, interagency partners, and overseas counterparts to share known details of the event(s), the impact to transportation, and mitigation measures being considered.
  - As an example, the majority of initial reporting on the Brussels bombings came from a TSAR based in Brussels who was at the airport that morning. TSARs and Regional Directors work with international partners to share best or proven international practices with domestic locations to enhance their security posture and overall efficiency. Another recent example is a trip by Dallas-Fort Worth International Airport personnel to meet with the Israeli Airport Authority at Ben Gurion International Airport in Tel Aviv to examine landside security countermeasures for possible adoption at the Dallas-Fort Worth Airport.
- As the U.S. lead on aviation security issues within ICAO, TSA actively seeks to influence decisions made within the broader organization, the ICAO Aviation Security Panel of Experts, and various internal and external working groups to enhance aviation security requirements, including through changes to the ICAO Standards and Recommended Practices. These outcomes, in turn, impact international implementation of effective aviation security measures.

~~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.~~

- TSA also engages with international stakeholder communities to share best practices and align our respective approaches of responding to evolving and emerging threats through the adoption of risk-based security practices. As part of the effort, TSA conducts threat and risk exchanges, leads efforts to develop a risk management training program, and identifies opportunities for coordinated engagement and assistance.

~~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.~~

Transportation Security Administration

U.S. Department of Homeland Security
Office of Security Operations
Arlington, VA 22202

October 12, 2016

From: Lalit Lal
Acting Branch Manager, Performance Management Branch
Security Operations

To: TSA Leadership

Subject: Measures of Effectiveness Report – September 2016

Performance Management is pleased to release the September Measures of Effectiveness (MOE) Report. This is the final report for the 2016 fiscal year.

Some key notes on the following metrics:

Ia – National Training Plan (NTP) on Pace: The NTP is not counting new hires who have on boarded on or after July 1, 2016. We understand that the training requirement of the plan would be difficult with our resources focused on the record summer travel season.

Ic – Annualized FTE including Overtime (excluding managers): For the month of September, Pay Periods 17 and 18 were used in the calculation.

Please find attached your Nationwide, Region, and Hub-specific MOE.

The final FY16 MOE post-publication call, will occur this Thursday, October 13th, 2016, following MOE publication at 14:00. I have included the call details below for all who would like to attend.

Measures of Effectiveness Report Conference Call – September 2016 Publication
Call Line (b)(6)
Participant Code (b)(6)

For additional information, Reference Guides, or supporting data see the Performance Management iShare, or contact the MOE Team at MOEHelpDesk@tsa.dhs.gov.

As always, please let us know if you have any questions or need anything else.

~~WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.~~

TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

	Period Actual	FY16 to Date	FY16 Target	% Effective	Weight
Workforce Readiness Measures that emphasize staffing, training, development, and preparedne required equipment and perform mission-essential functions.				92.4%	30.0
Ia - National Training Plan (NTP) on Pace	82.1%	82.1%	90.0%	91.2%	10.0
Ib - Annual Proficiency Review (APR) Variance	12.3%	12.3%	15.0%	100%*	5.0
Ic - Annualized FTE including Overtime (excluding managers)	43,389.2	42,420.8	42,257.1	100.4%	5.0
Id - Unscheduled Absences	3.2%	3.5%	2.5%		5.0
Ie - Traumatic Injury Hours	4,057.0	40,853.8	49,770.2	100%*	5.0

	Period Actual	FY16 to Date	FY16 Target	% Effective	Weight
Workforce Performance Measures that reflect the effectiveness of the workforce in				(b)(3):49 U.S.C. § 114(r)	30.0
IIa - Selectee Find Rate (TSA Miss)**	(b)(3):49 U.S.C. § 114(r)				
IIb - On Screen Alarm Resolution Protocol (OSARP)	(b)				
IIc - Threat Image Projection (TIP	(b)				
IId - ASAP Detection Rate					

	Period Actual	FY16 to Date	FY16 Target	% Effective	Weight
System Readiness Measures that demonstrate that appropri available to perform the mission for whic				(b)(3):49 U.S.C. § 114(r)	20.0
IIIa - Mission Essential Level: Detect	(b)(3):49 U.S.C. § 114(r)				
IIIb - Mission Essential Level: Deter					
IIIc - Compliance Finding Resolution	84.0%	84.0%	100.0%		5.0
IIId - Equipment Downtime	0.6%	0.6%	1.0%	100%*	2.5

	Period Actual	FY16 to Date	FY16 Target	% Effective	Weight
System Performance Measures that reflect the overall effectiveness of the system in achieving system detection standards and the desired effects of deter, detect, disrupt.				(b)(3):49 U.S.C. § 114(r)	
IVa - Throughput Vulnerability Hours	(b)(3):49 U.S.C. § 114(r)				
IVb - Controlled Security Incidents per 100K PAX	0.59	0.61	0.56	93.0%	5.0
IVc - TSA PreCheck Disqualification Processing Timeliness	96.6%	93.2%	100.0%	93.2%	7.5

Overall Effectiveness (b)(3):49 U.S.C. § 114(r)

* This metric's % effective has been capped at 100%
** This metric's target may change if an airport has <200 selectees

Default Color Coding (except for Ic and IIa): 85% - 95% >95%

Please see the MOE Reference Guide for additional metric-specific information

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-trained on password-protected servers.~~

TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

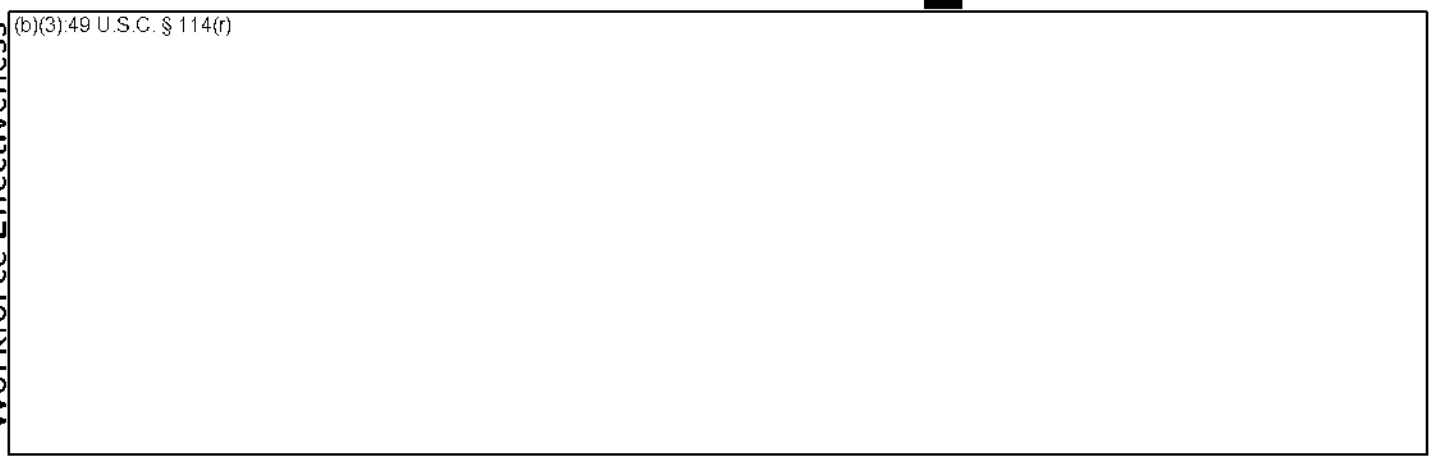
Nationwide

September 2016

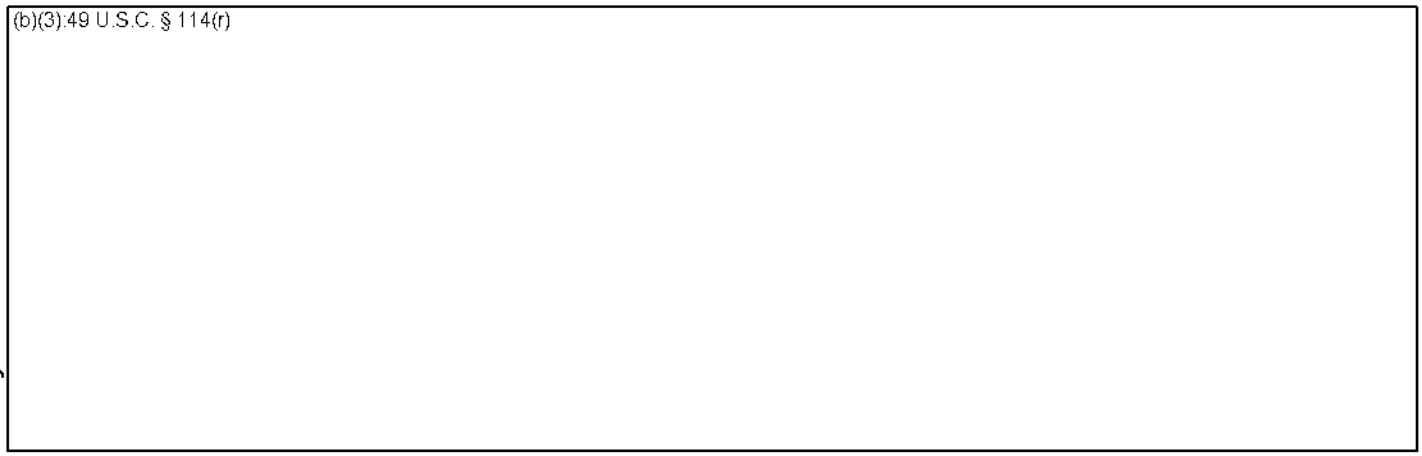
Readiness

Performance

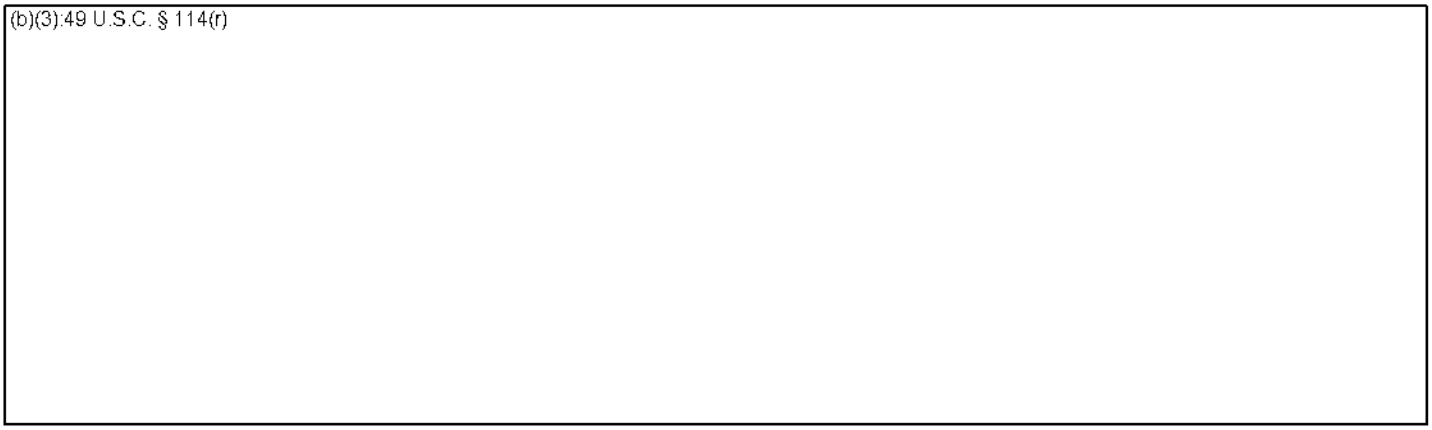
Workforce Effectiveness



System Effectiveness



Overall Effectiveness



Overall % Effective - Period Actual

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed files on password-protected servers.

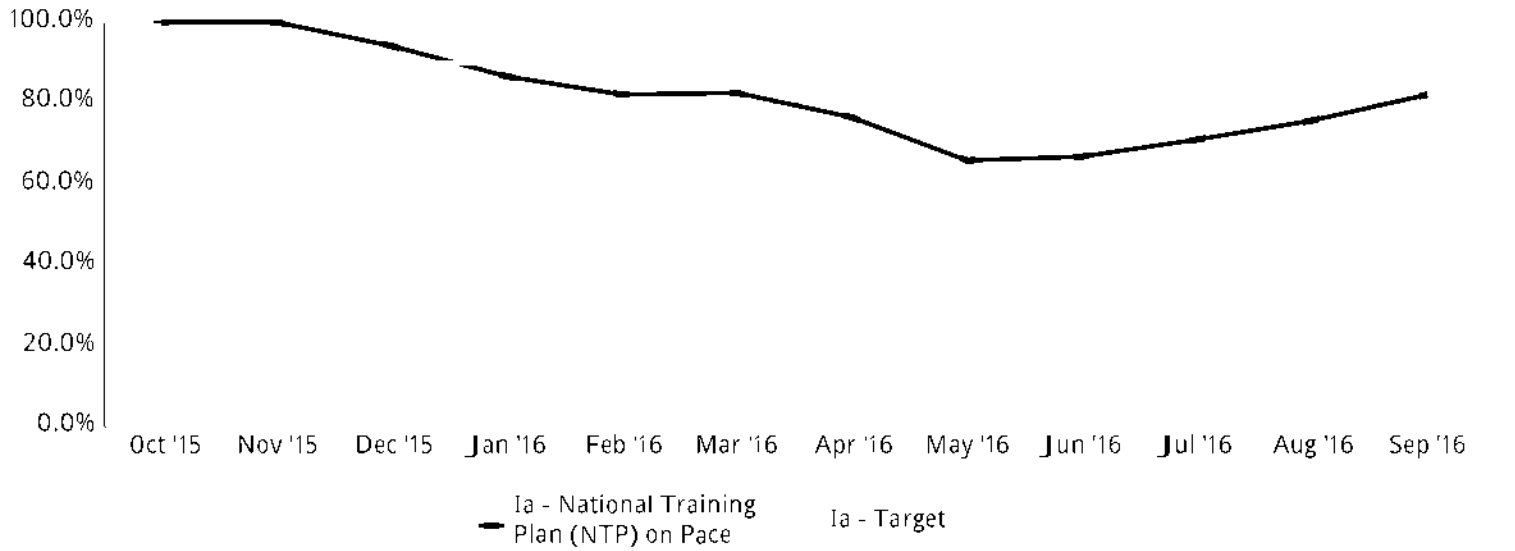
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

Ia - National Training Plan (NTP) on Pace



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	53.8%	90.0%	59.8%	14.7%
Region 2	93.0%	90.0%	103.3%	16.3%
Region 3	75.8%	90.0%	84.2%	15.2%
Region 4	91.6%	90.0%	101.8%	10.8%
Region 5	65.4%	90.0%	72.7%	9.4%
Region 6	94.2%	90.0%	104.7%	21.1%
Region 7	93.1%	90.0%	103.4%	12.5%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

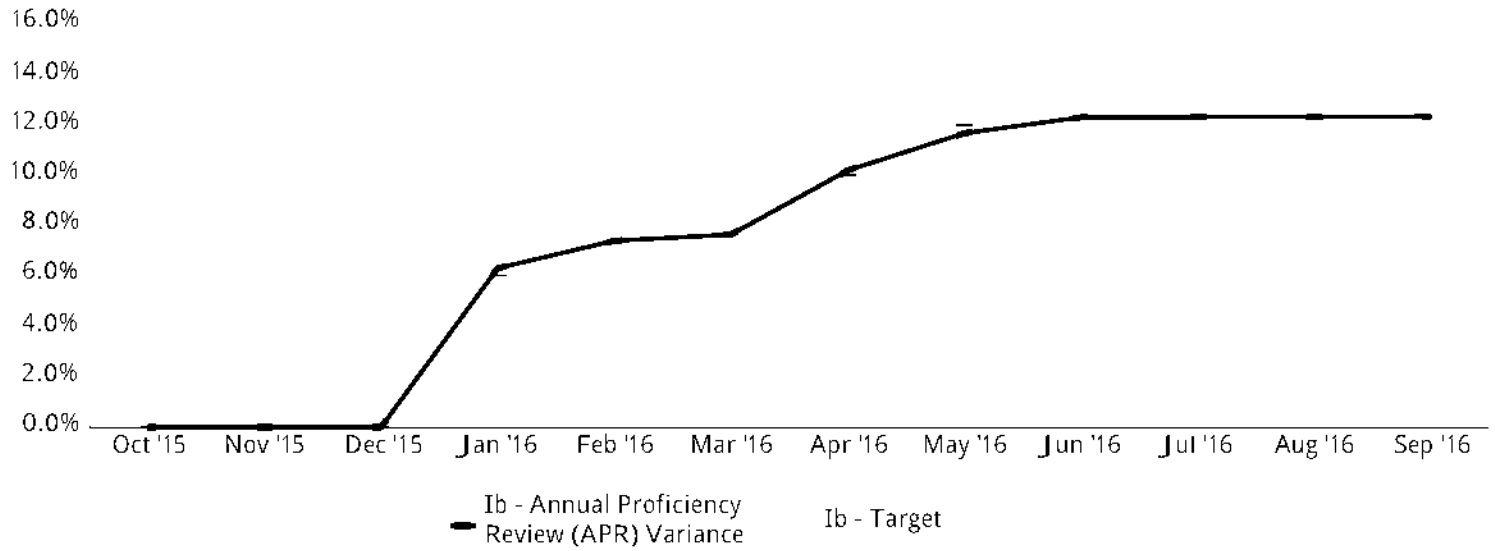
FY16 Measures of Effectiveness

Nationwide

September 2016

Ib- Annual Proficiency Review (APR) Variance

[redacted]



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	13.6%	15.0%	110.4%	13.9%
Region 2	11.7%	15.0%	128.6%	16.5%
Region 3	11.7%	15.0%	128.6%	15.9%
Region 4	11.2%	15.0%	134.4%	11.2%
Region 5	11.6%	15.0%	129.0%	9.2%
Region 6	12.2%	15.0%	122.7%	20.7%
Region 7	14.5%	15.0%	103.5%	12.6%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password protected. Electronically transmitted or maintained on password-protected servers.

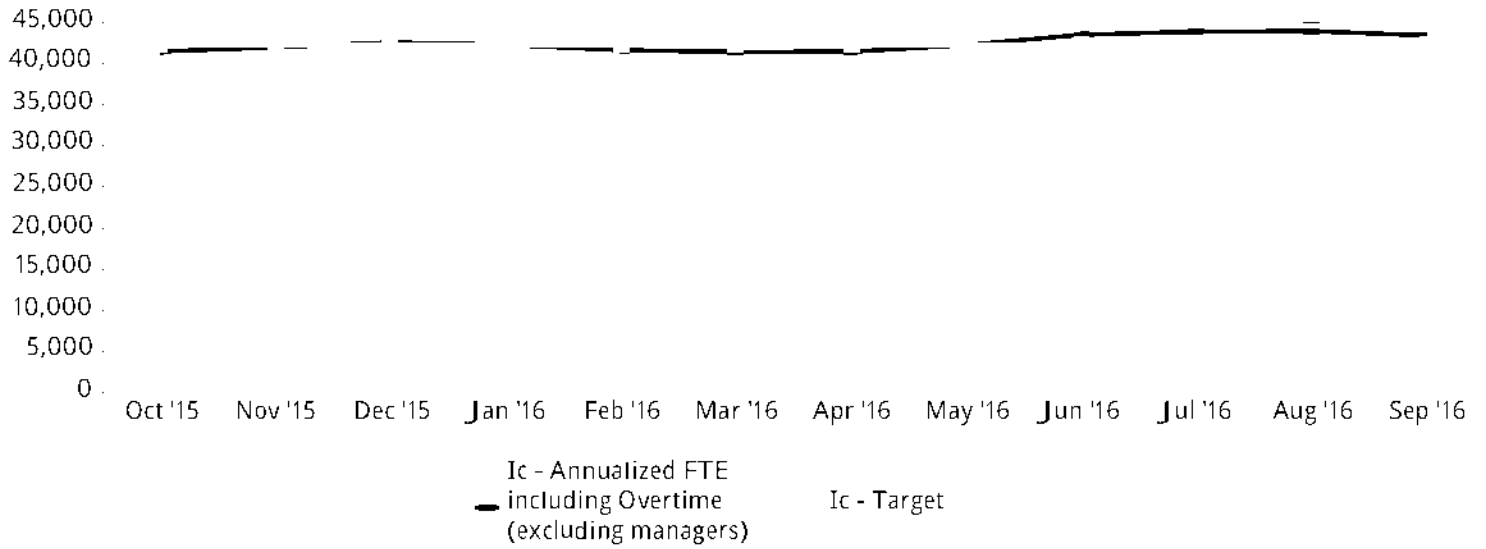
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

Ic- Annualized FTE including Overtime (excluding managers)



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	6,395.5	6,287.0	101.7%	15.1%
Region 2	7,073.2	7,015.2	100.8%	16.7%
Region 3	6,238.4	6,297.8	99.1%	14.7%
Region 4	4,812.6	4,821.6	99.8%	11.3%
Region 5	4,051.6	4,104.3	98.7%	9.6%
Region 6	8,224.3	8,205.2	100.2%	19.4%
Region 7	5,625.2	5,526.0	101.8%	13.3%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be safeguarded, protected, electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

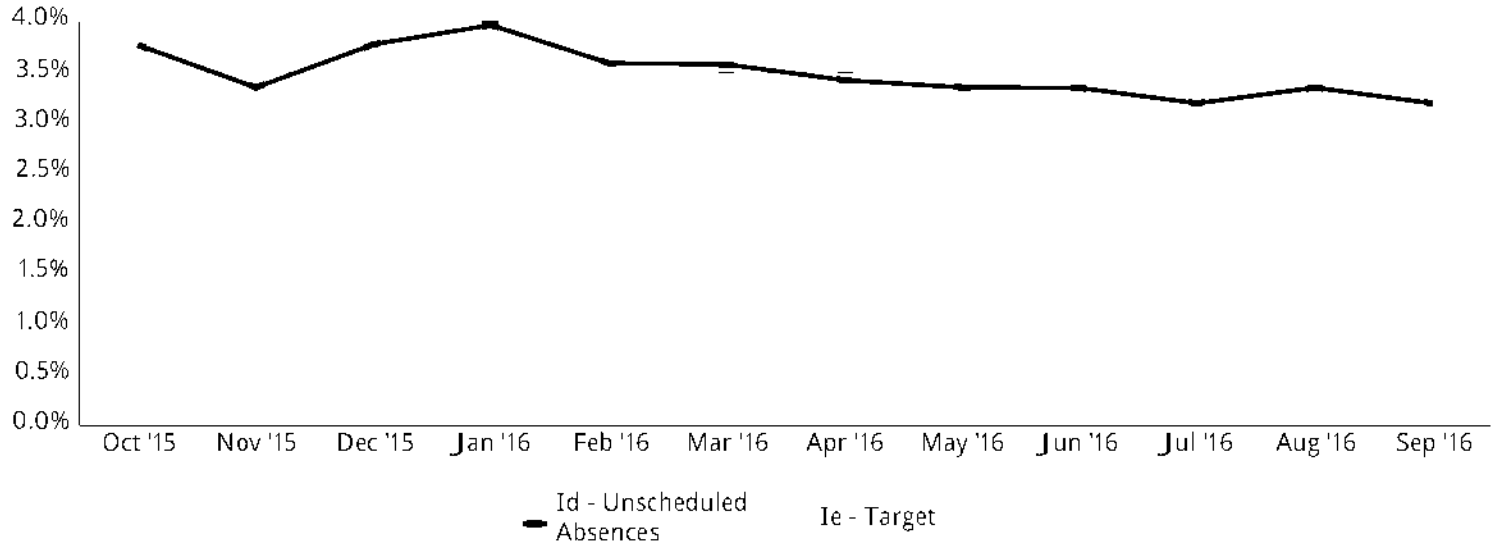
FY16 Measures of Effectiveness

Nationwide

September 2016

Id- Unscheduled Absences

[redacted]



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	4.6%	3.2%	69.2%	14.9%
Region 2	3.8%	2.5%	66.4%	15.5%
Region 3	3.4%	2.4%	71.0%	15.5%
Region 4	3.4%	2.5%	73.5%	11.1%
Region 5	2.7%	2.1%	75.4%	9.4%
Region 6	3.0%	2.4%	79.9%	21.2%
Region 7	3.4%	2.6%	74.7%	12.4%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

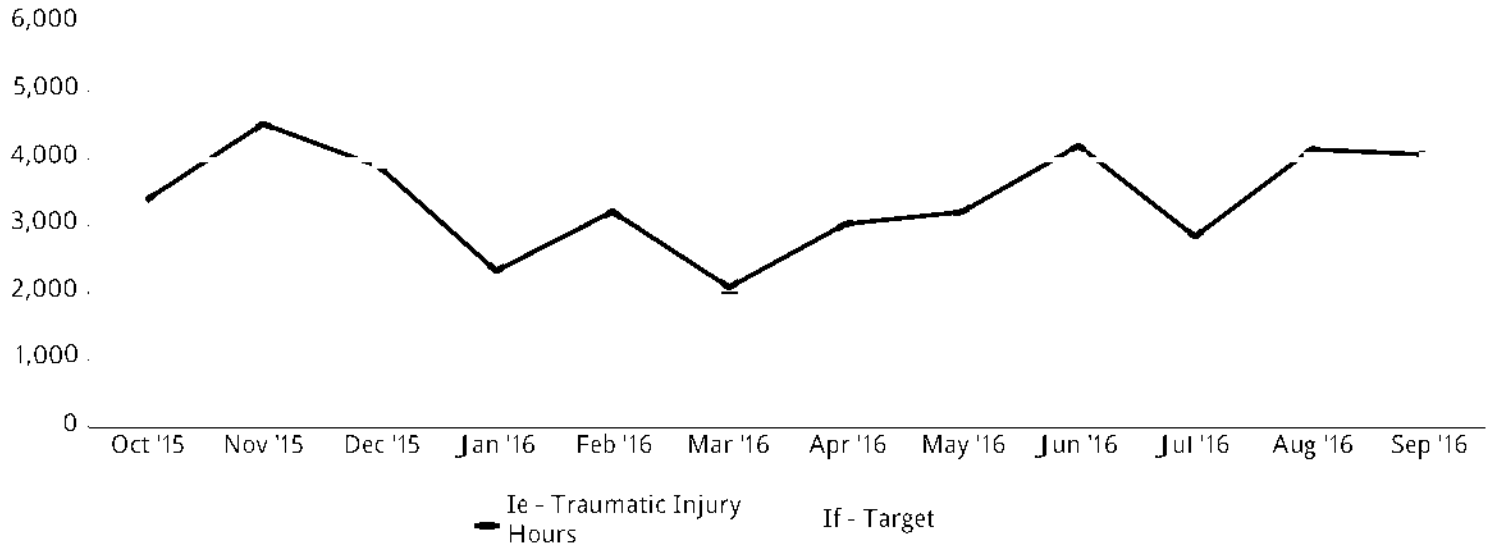
FY16 Measures of Effectiveness

Nationwide

September 2016

Ie- Traumatic Injury Hours

[redacted]



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	6,122.5	10,153.8	165.8%	15.0%
Region 2	10,216.0	10,839.4	106.1%	25.0%
Region 3	4,064.8	6,428.8	158.2%	9.9%
Region 4	3,507.0	4,238.5	120.9%	8.6%
Region 5	2,320.5	2,955.8	127.4%	5.7%
Region 6	6,041.8	5,645.2	93.4%	14.8%
Region 7	8,581.3	9,508.7	110.8%	21.0%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password protected. Electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

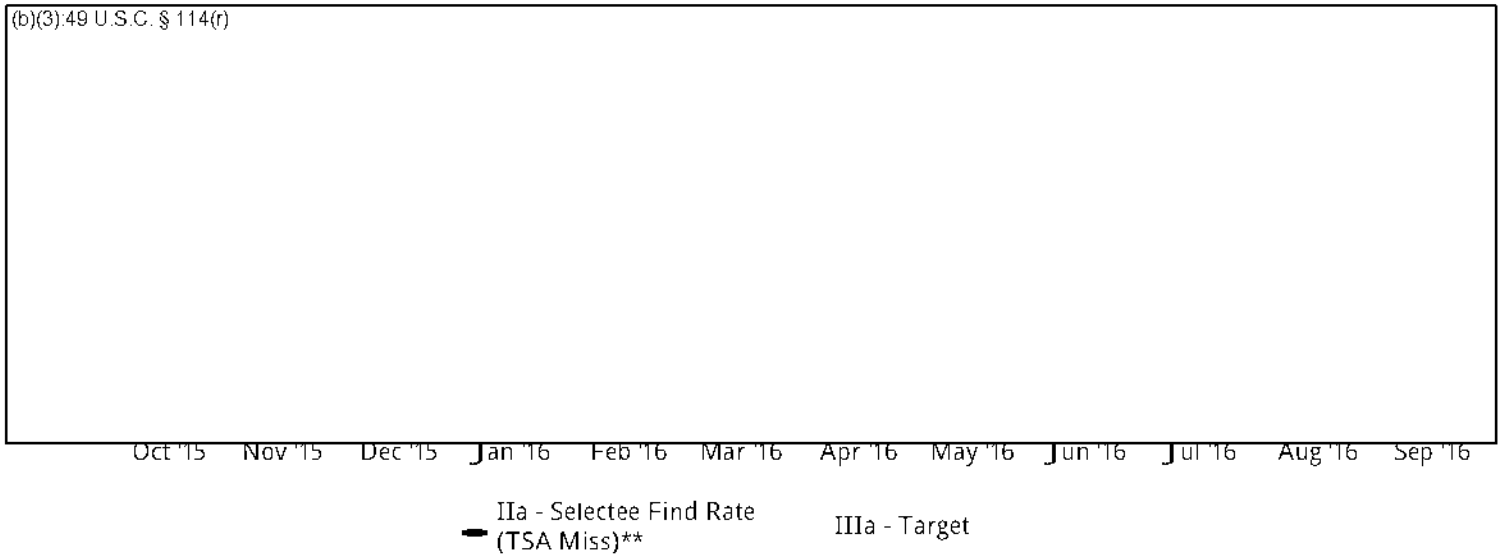
FY16 Measures of Effectiveness

Nationwide

September 2016

IIa - Selectee Find Rate (TSA Miss)

[redacted]



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password protected. Electronically transmitted or mailed on password-protected servers.

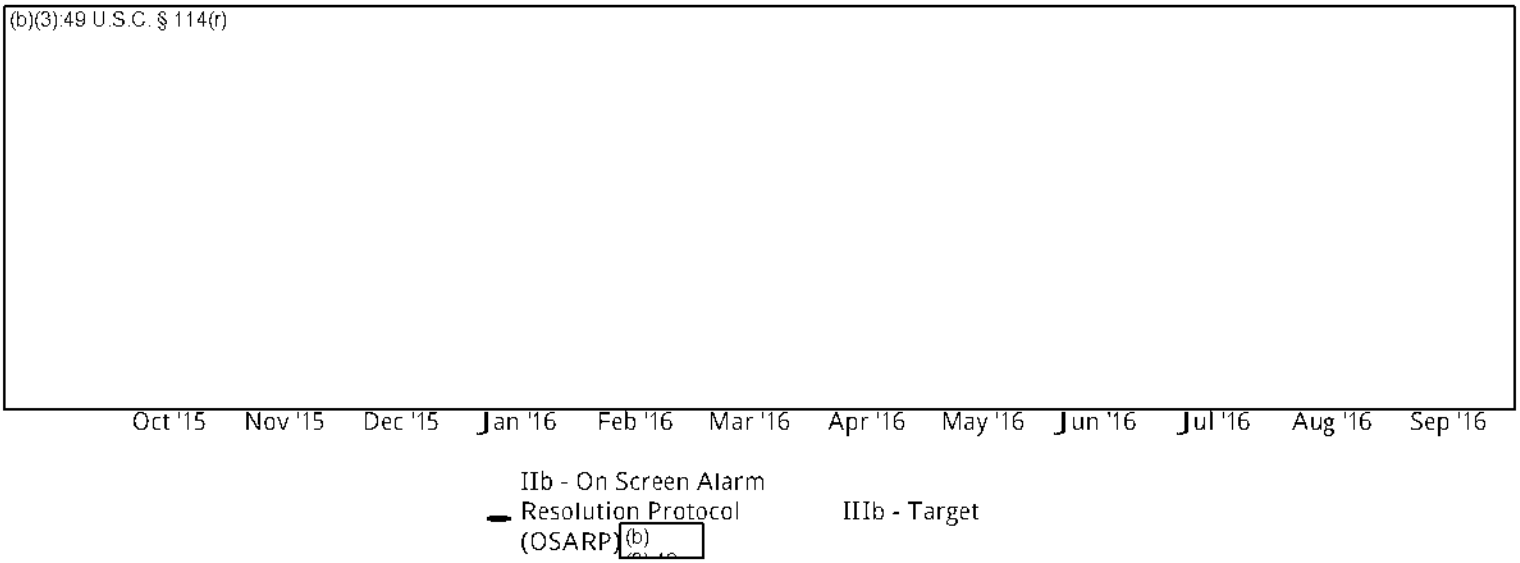
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

IIb - On Screen Alarm Resolution Protocol (OSARP) (b)(3):49 U.S.C. § [redacted]



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

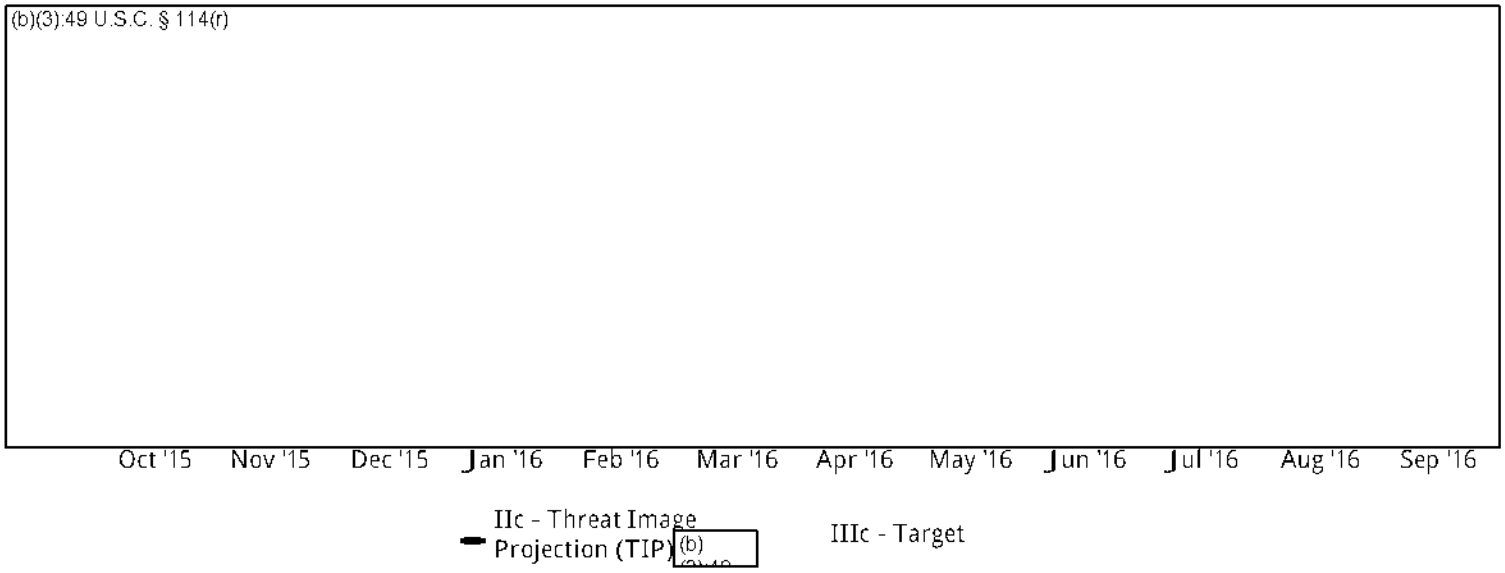
FY16 Measures of Effectiveness

Nationwide

September 2016

IIc - Threat Image Projection (TIP) (b)(3):49 U.S.C. §

[redacted]



Region Breakout

Region
Region 1
Region 2
Region 3
Region 4
Region 5
Region 6
Region 7

(b)(3):49 U.S.C. § 114(r)

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-tained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

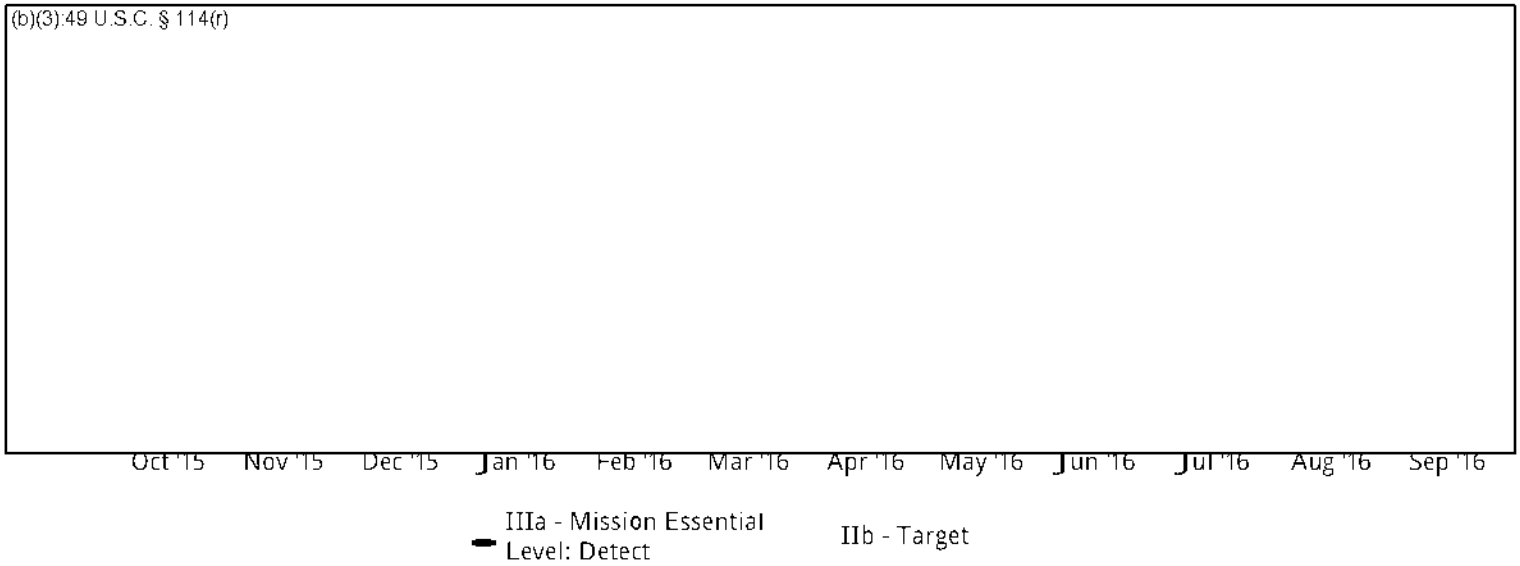
FY16 Measures of Effectiveness

Nationwide

September 2016

IIIa - Mission Essential Level: Detect

[redacted]



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be safeguarded, protected, electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide September 2016

IIIb - Mission Essential Level: Deter

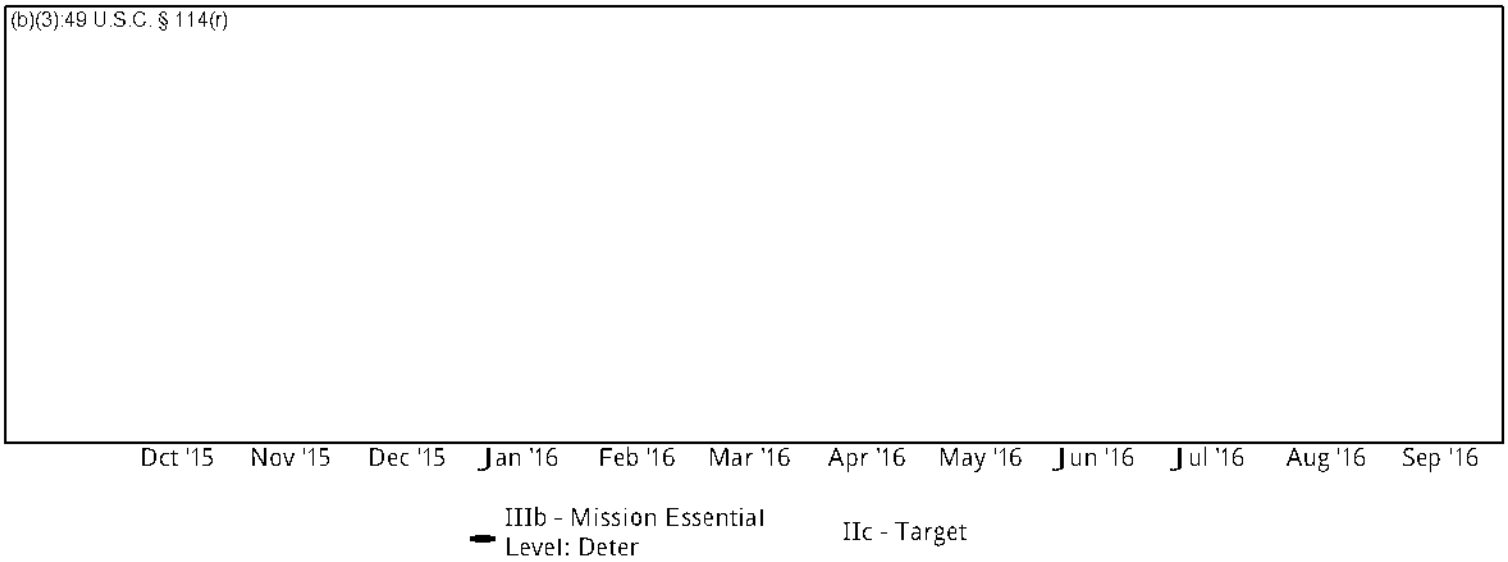
[redacted]

(b)(3):49 U.S.C. § 114(r)

Dct '15 Nov '15 Dec '15 Jan '16 Feb '16 Mar '16 Apr '16 May '16 Jun '16 Jul '16 Aug '16 Sep '16

IIIb - Mission Essential Level: Deter

IIc - Target



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected if electronically transmitted or maintained on password-protected servers.~~

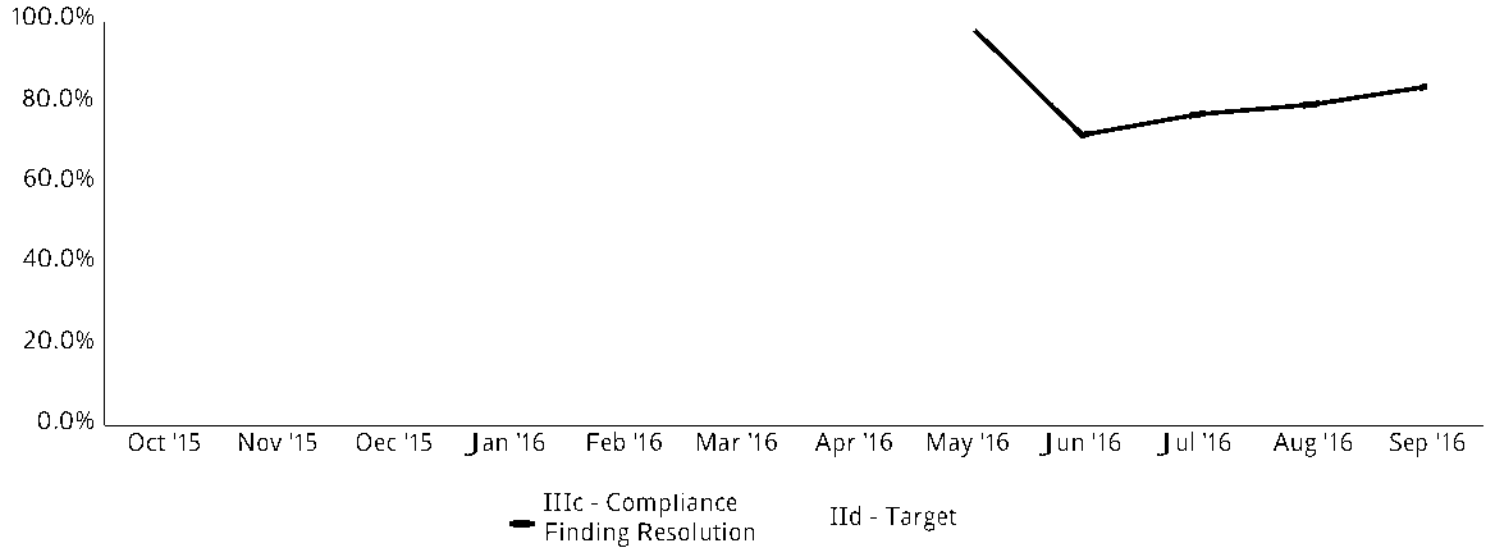
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

IIIc - Compliance Finding Resolution



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	96.5%	100.0%	96.5%	20.2%
Region 2	80.9%	100.0%	80.9%	23.5%
Region 3	74.8%	100.0%	74.8%	18.2%
Region 4	74.6%	100.0%	74.6%	7.3%
Region 5	75.5%	100.0%	75.5%	7.8%
Region 6	90.4%	100.0%	90.4%	14.8%
Region 7	87.8%	100.0%	87.8%	8.1%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

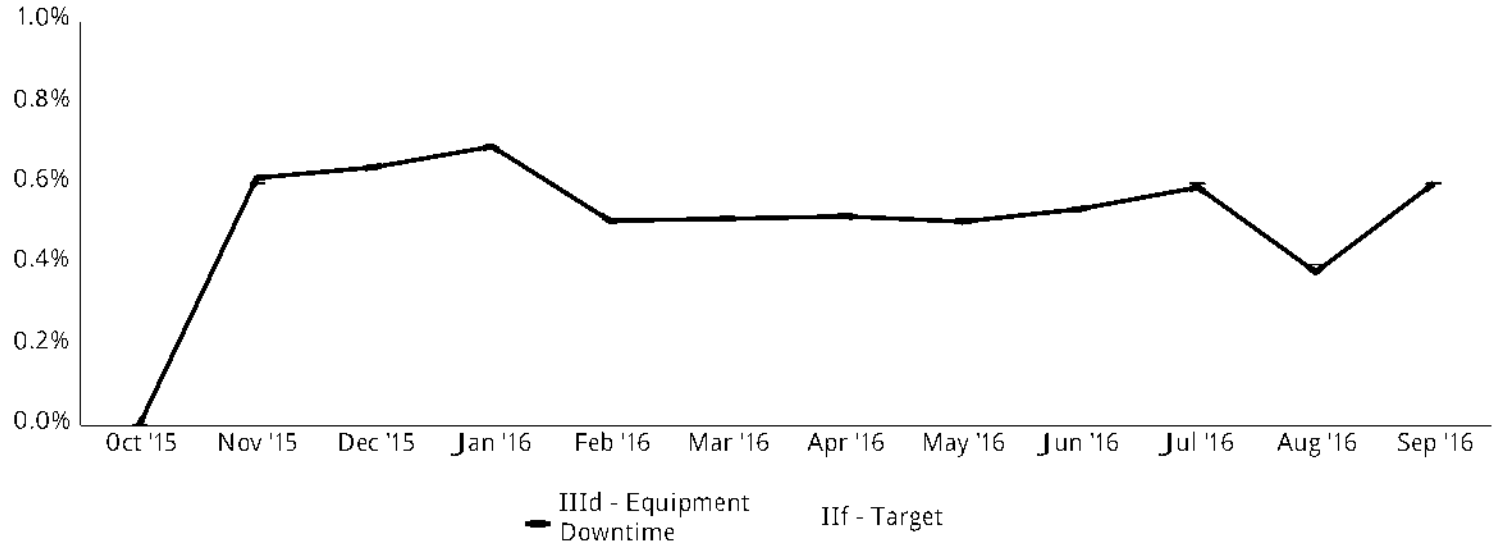
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

IIId - Equipment Downtime



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	0.7%	1.0%	146.3%	13.6%
Region 2	0.5%	1.0%	185.4%	17.2%
Region 3	0.4%	1.0%	262.4%	14.2%
Region 4	0.5%	1.0%	183.7%	10.4%
Region 5	0.5%	1.0%	199.5%	10.8%
Region 6	0.7%	1.0%	146.9%	20.0%
Region 7	0.5%	1.0%	202.9%	13.8%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

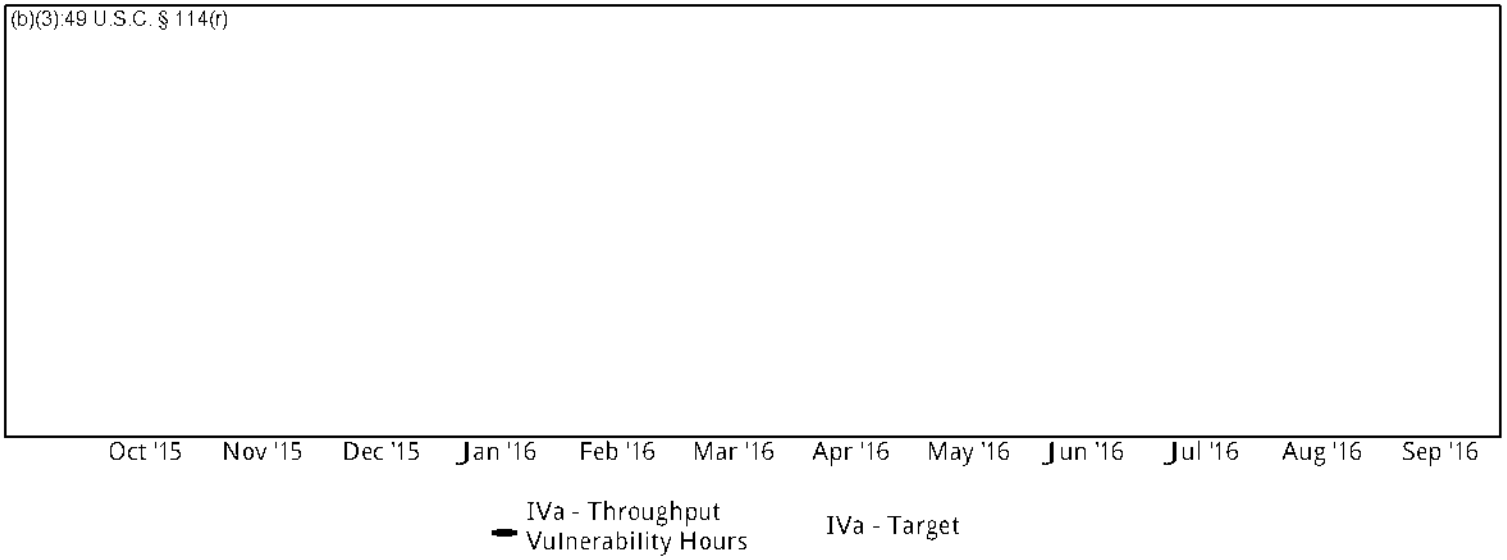
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

IVa - Throughput Vulnerability Hours



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-shared on password-protected servers.~~

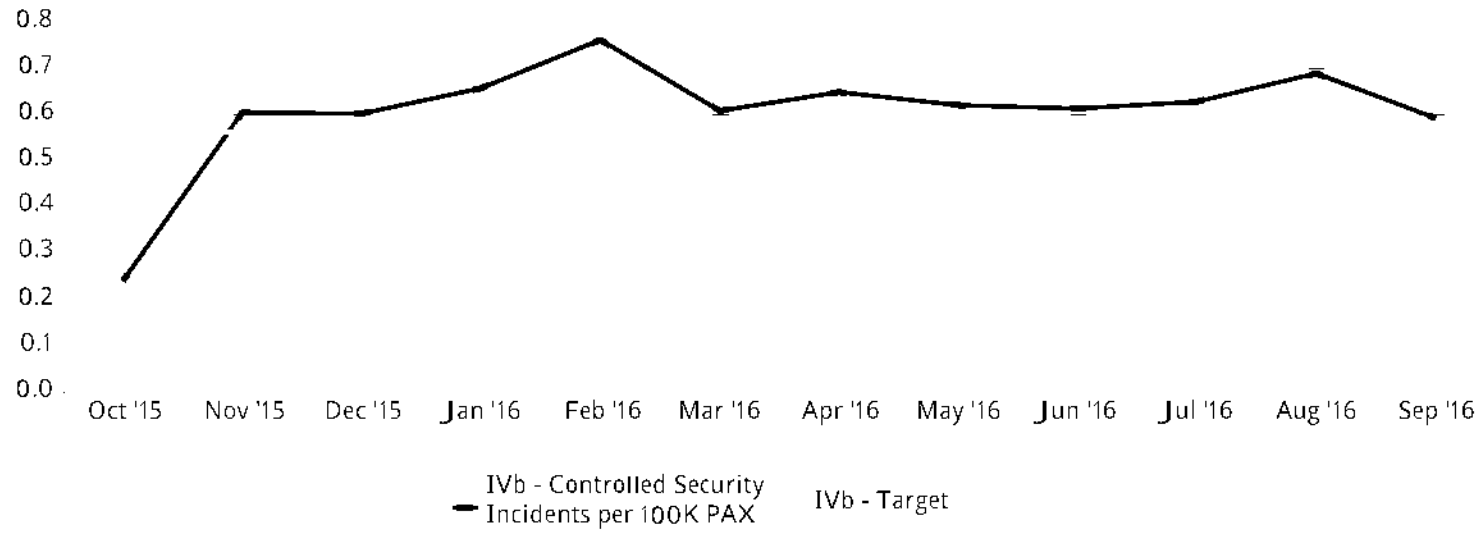
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

IVb - Controlled Security Incidents per 100K Pax



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	0.49	0.52	106.5%	14.3%
Region 2	0.53	0.52	98.4%	17.0%
Region 3	0.91	0.70	77.8%	14.3%
Region 4	0.49	0.51	104.6%	10.6%
Region 5	1.05	0.75	71.2%	9.2%
Region 6	0.48	0.51	106.1%	22.6%
Region 7	0.49	0.51	104.0%	11.9%

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be safeguarded, protected, electronically transmitted or maintained on password-protected servers.~~

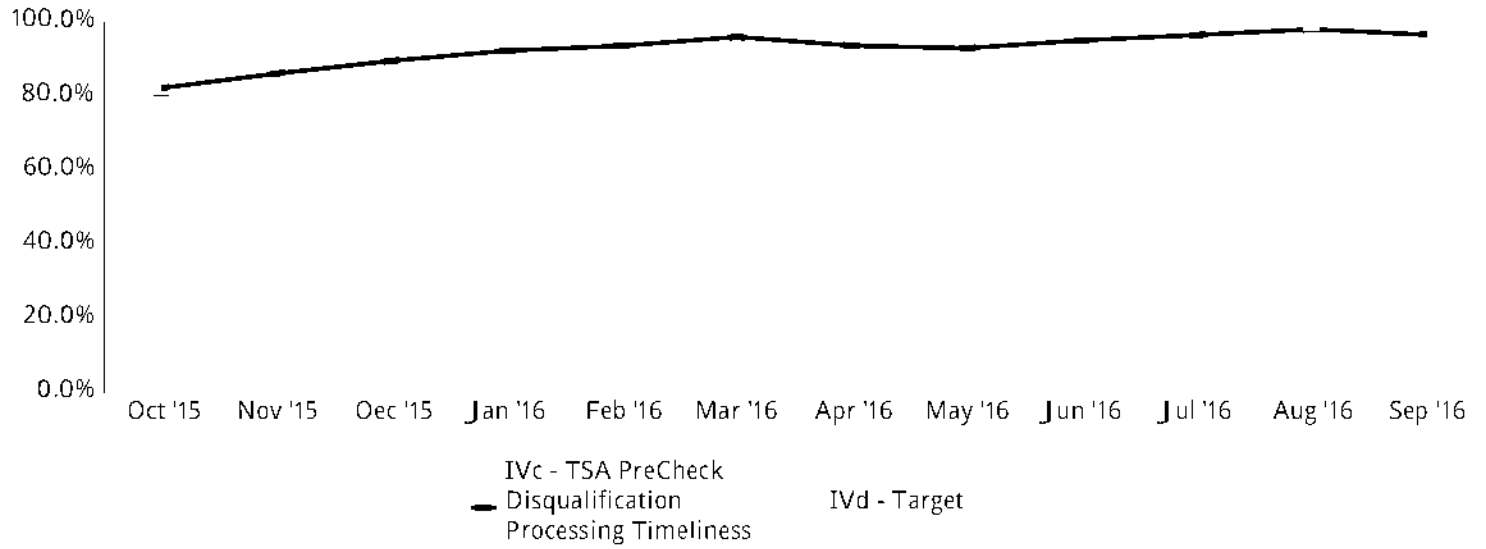
TRANSPORTATION SECURITY ADMINISTRATION

FY16 Measures of Effectiveness

Nationwide

September 2016

IVc - PreCheck Disqualification Program Processing Timeliness



Region Breakout

Region	FY16 to Date	FY16 Target	% Effective	Contribution to Nation
Region 1	91.6%	100.0%	91.6%	3.4%
Region 2	94.3%	100.0%	94.3%	15.6%
Region 3	94.7%	100.0%	94.7%	14.1%
Region 4	91.7%	100.0%	91.7%	20.0%
Region 5	93.9%	100.0%	93.9%	17.6%
Region 6	93.4%	100.0%	93.4%	16.0%
Region 7	91.5%	100.0%	91.5%	13.2%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

Transportation Security Administration

U.S. Department of Homeland Security
Office of Security Operations
Arlington, VA 22202

December 13, 2016

From: Benjamin Sears
Branch Manager, Performance Management Branch
Security Operations

To: TSA Leadership

Subject: FY17 Measures of Effectiveness Report – November 2016

Performance Management is pleased to release the November Measures of Effectiveness (MOE) Report.

Some key notes on the following metrics:

Ic – Annualized FTE including Overtime (excluding managers): FTE data has been added through PP22 to include 20 and 21 for October 2016.

Ie – Traumatic Injury Hours: FTE data has been added through PP22 to include 20 and 21 for October 2016.

IIc – Threat Image Projection (TIP (b)(3):49 U.S.C. § 1 Officers seeing (b)(3):49 U.S.C. § 114(r) were removed from the MOE measure in order to match the latest TIP OD which goes into effect April 1, 2017. Previous MOEs reflected those officers seeing greater than 10 TIP images. The TIP measure includes only fiscal year data, previous data has been removed as it did fall inside the fiscal.

IIIc – Compliance Finding Resolution: The methodology has changed for this metric; thus, data has been cleared and will begin showing on the February publication. Guidance on the new metric will be messaged through your AFSD-I's.

Please find attached your Nationwide, Region, and Hub-specific MOE.

The MOE post-publication call will occur this Thursday, December 15th, 2016, following MOE publication at 14:00. I have included the call details below for all who would like to attend.

Measures of Effectiveness Report Conference Call – November 2016 Publication
Call Line: (b)(6)
Participant Code: (b)(6)

~~WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.~~

For additional information, Reference Guides, or supporting data see the Performance Management iShare, or contact the MOE Team at MOEHelpDesk@tsa.dhs.gov. As always, please let us know if you have any questions or need anything else.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
Workforce Readiness Measures that emphasize staffing, training, development, and preparedne required equipment and perform mission-essential functions.				87.6%	30.0
Ia - National Training Plan (NTP) on Pace	67.4%	67.4%	90.0%		10.0
Ib - Annual Proficiency Review (APR) Variance	12.4%	12.4%	15.0%	100%*	5.0
Ic - Annualized FTE including Overtime (excluding managers)	43,988.6	43,833.2	44,157.6	99.3%	5.0
Id - Unscheduled Absences	3.1%	3.3%	2.5%		5.0
Ie - Traumatic Injury Hours	1,795.0	5,173.0	5,979.3	100%*	5.0

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
Workforce Performance Measures that reflect the effectiveness of the workforce in				(b)(3):49 U.S.C. § 114(r)	30.0
IIa - Selectee Find Rate (TSA Miss)**	(b)(3):49 U.S.C. § 114(r)				10.0
IIb - On Screen Alarm Resolution Protocol (OSARP	(b)				10.0
IIc - Threat Image Projection (TIP	(b)				10.0
IId - ASAP Detection Rate	Classified: data can be found in TRACE				

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
System Readiness Measures that demonstrate that appropri available to perform the mission for whic				(b)(3):49 U.S.C. § 114(r)	20.0
IIIa - Mission Essential Level: Detect	(b)(3):49 U.S.C. § 114(r)				5.0
IIIb - Mission Essential Level: Deter					7.5
IIIc - Compliance Finding Resolution	100.0%	100.0%	100.0%	100.0%	5.0
IIId - Equipment Downtime	0.6%	0.5%	1.0%	100%*	2.5

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
System Performance Measures that reflect the overall effectiveness of the system in achieving system detection standards and the desired effects of deter, detect, disrupt.				(b)(3):49 U.S.C. § 114 (r)	
IVa - Throughput Vulnerability Hours	(b)(3):49 U.S.C. § 114(r)				
IVb - Controlled Security Incidents per 100K PAX					
IVc - TSA PreCheck Disqualification Processing Timeliness	98.1%	97.5%	100.0%	97.5%	7.5

Overall Effectiveness

95.8%

* This metric's % effective has been capped at 100%
** This metric's target may change if an airport has <200 selectees

Default Color Coding (except for Ic and IIa): 85% - 95% >95%

Please see the MOE Reference Guide for additional metric-specific information

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or retrieved on password-protected servers.~~

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

Readiness Performance

Workforce Effectiveness

(b)(3):49 U.S.C. § 114(r)

System Effectiveness

(b)(3):49 U.S.C. § 114(r)

Overall Effectiveness

(b)(3):49 U.S.C. § 114(r)

Oct '16

Nov '16

Overall % Effective - Period Actual

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

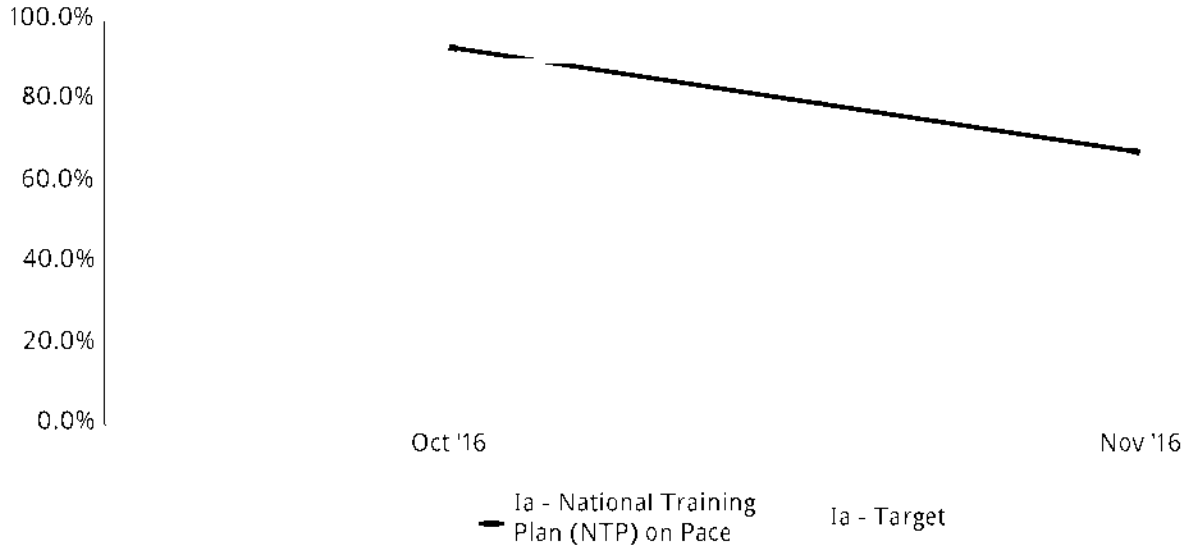
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

Ia - National Training Plan (NTP) on Pace



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	74.1%	90.0%	82.3%	14.7%
Region 2	65.2%	90.0%	72.5%	16.4%
Region 3	67.7%	90.0%	75.3%	15.3%
Region 4	63.1%	90.0%	70.1%	10.8%
Region 5	68.8%	90.0%	76.5%	9.5%
Region 6	63.7%	90.0%	70.8%	20.7%
Region 7	70.9%	90.0%	78.8%	12.5%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

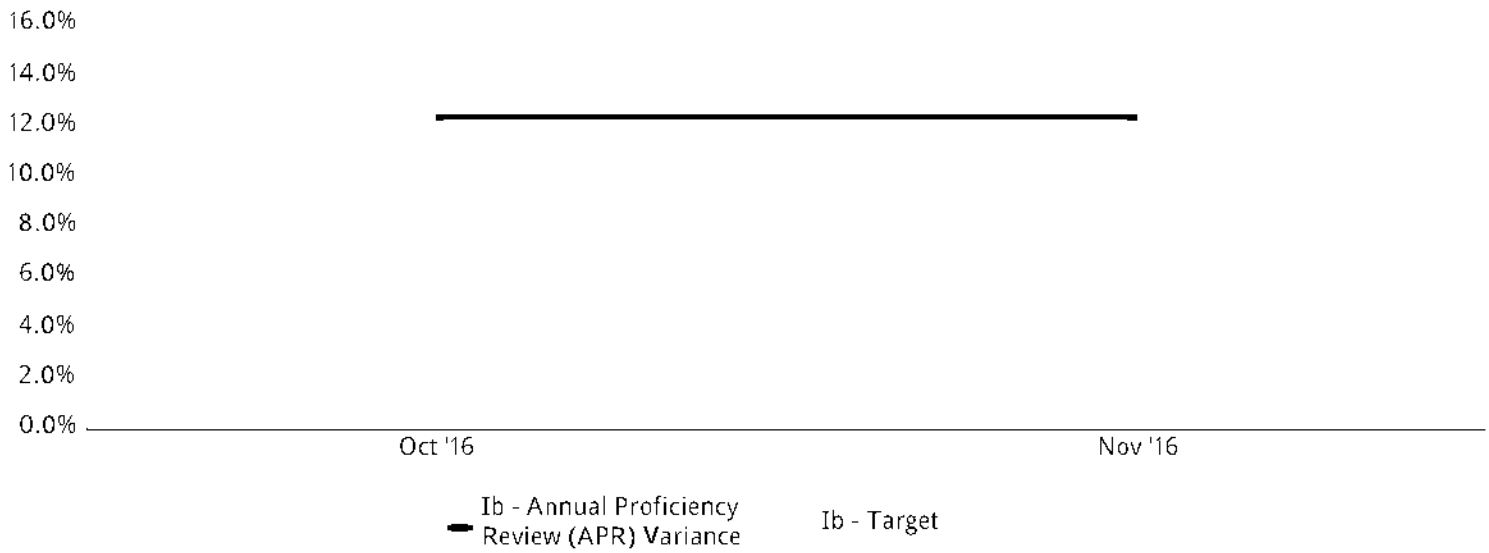
FY17 Measures of Effectiveness

Nationwide

November 2016

Ib- Annual Proficiency Review (APR) Variance

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	13.8%	15.0%	108.7%	14.2%
Region 2	11.8%	15.0%	127.4%	16.5%
Region 3	11.7%	15.0%	128.1%	15.8%
Region 4	11.1%	15.0%	134.8%	11.2%
Region 5	11.6%	15.0%	129.0%	9.1%
Region 6	12.2%	15.0%	123.0%	20.7%
Region 7	14.5%	15.0%	103.7%	12.5%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or received on password-protected servers.

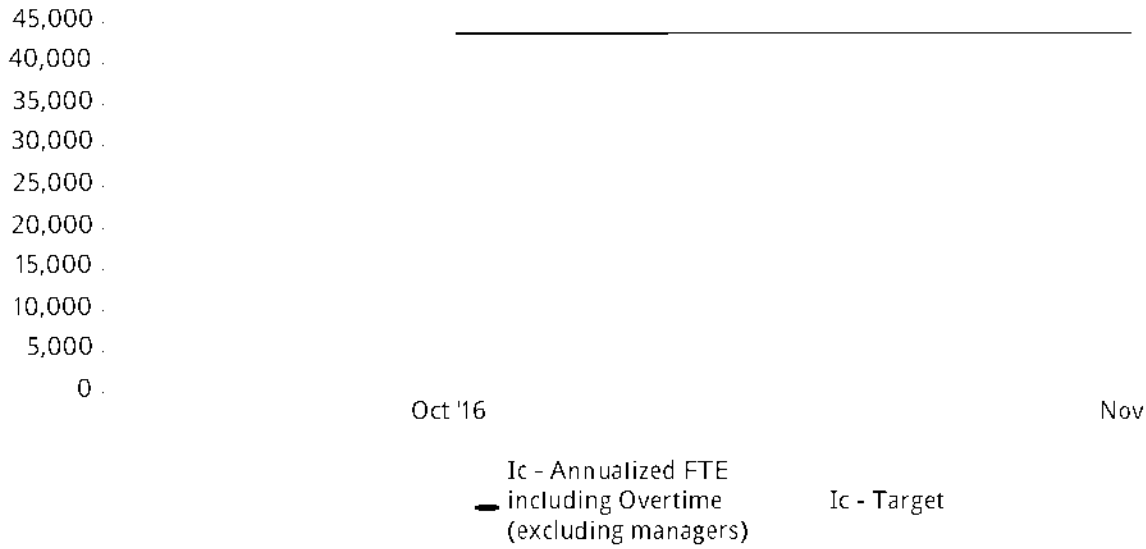
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

Ic- Annualized FTE including Overtime (excluding managers)



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	6,622.6	6,588.7	100.5%	15.1%
Region 2	7,212.7	7,239.7	99.6%	16.5%
Region 3	6,597.5	6,600.3	100.0%	15.1%
Region 4	4,938.2	4,898.4	100.8%	11.3%
Region 5	4,244.6	4,384.8	96.8%	9.7%
Region 6	8,494.1	8,703.7	97.6%	19.4%
Region 7	5,723.6	5,742.1	99.7%	13.1%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be safeguarded, protected, electronically transmitted or mailed on password protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

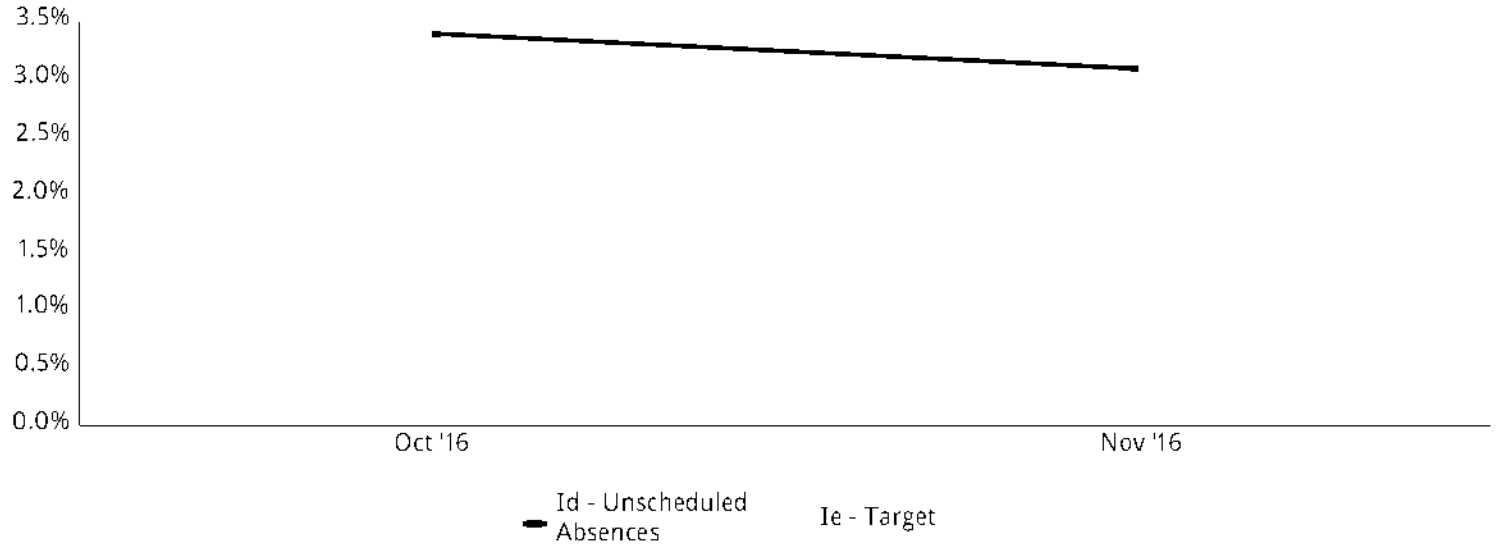
FY17 Measures of Effectiveness

Nationwide

November 2016

Id- Unscheduled Absences

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	4.1%	3.1%	74.8%	14.9%
Region 2	3.7%	2.6%	70.1%	15.5%
Region 3	3.0%	2.4%	80.2%	15.7%
Region 4	3.1%	2.4%	76.9%	11.0%
Region 5	2.7%	2.2%	80.2%	9.4%
Region 6	2.9%	2.3%	80.2%	21.4%
Region 7	3.2%	2.4%	76.0%	12.1%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed emails on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

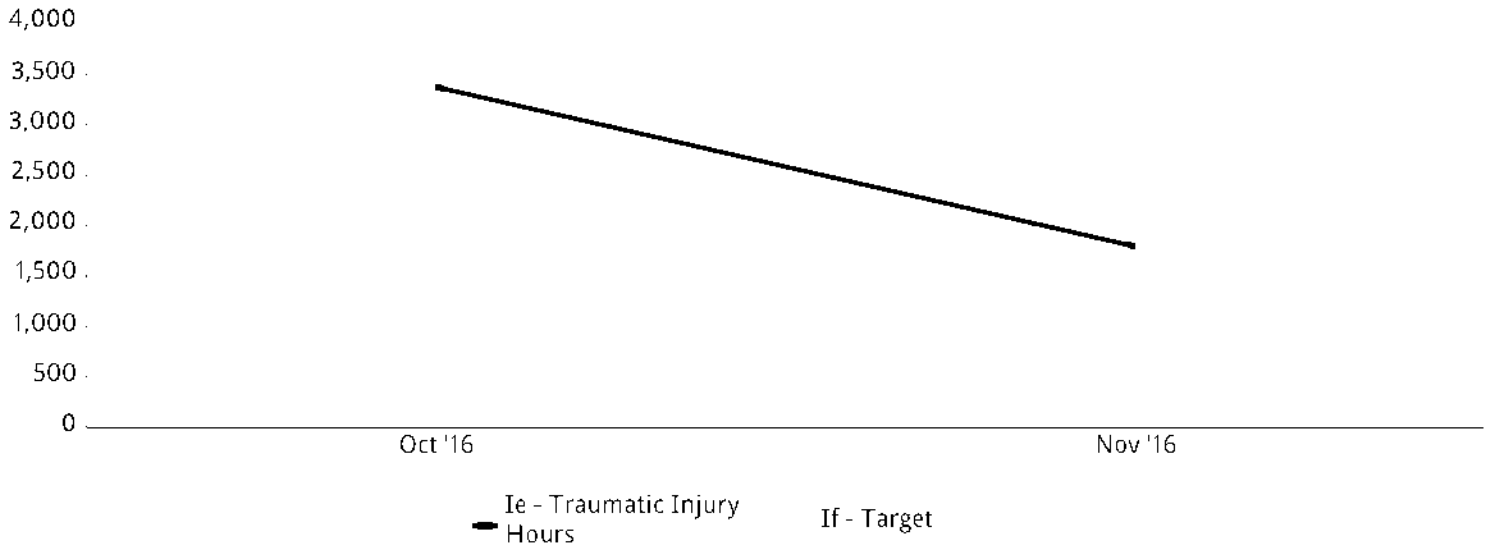
FY17 Measures of Effectiveness

Nationwide

November 2016

Ie- Traumatic Injury Hours

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	400.0	843.2	210.8%	7.7%
Region 2	1,285.0	550.8	42.9%	24.8%
Region 3	884.0	1,273.0	144.0%	17.1%
Region 4	220.0	620.4	282.0%	4.3%
Region 5	617.0	1,399.5	226.8%	11.9%
Region 6	906.0	698.1	77.1%	17.5%
Region 7	861.0	594.2	69.0%	16.6%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

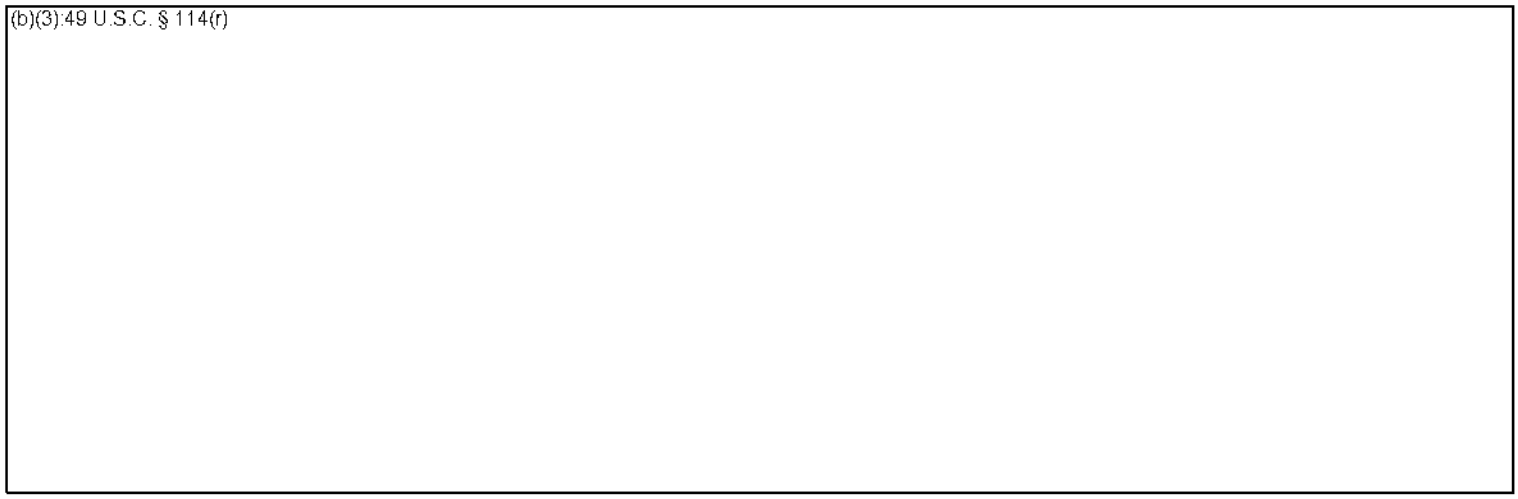
Nationwide

November 2016

IIa - Selectee Find Rate (TSA Miss)

[redacted]

(b)(3):49 U.S.C. § 114(r)



IIa - Selectee Find Rate (TSA Miss)**

IIIa - Target

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IIb - On Screen Alarm Resolution Protocol (OSARP) (b)(3):49 U.S.C. § [redacted]

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IIc - Threat Image Projection (TIP

(b)(3):49 U.S.C. § 11

[redacted]

(b)(3):49 U.S.C. § 114(r)

Oct '16

Nov '16

IIc - Threat Image Projection (TIP)

(b)(3):49

IIIc - Target

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be safeguarded, protected, electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IIIa - Mission Essential Level: Detect

[redacted]

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IIIb - Mission Essential Level: Deter

[redacted]

(b)(3):49 U.S.C. § 114(r)

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be safeguarded, protected, electronically transmitted or mailed only on password-protected servers.~~

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IIIc - Compliance Finding Resolution

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	100.0%	100.0%	100.0%	0.0%
Region 2	100.0%	100.0%	100.0%	0.0%
Region 3	100.0%	100.0%	100.0%	0.0%
Region 4	100.0%	100.0%	100.0%	0.0%
Region 5	100.0%	100.0%	100.0%	0.0%
Region 6	100.0%	100.0%	100.0%	0.0%
Region 7	100.0%	100.0%	100.0%	0.0%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password protected. Electronically transmitted or retrieved on password-protected servers.

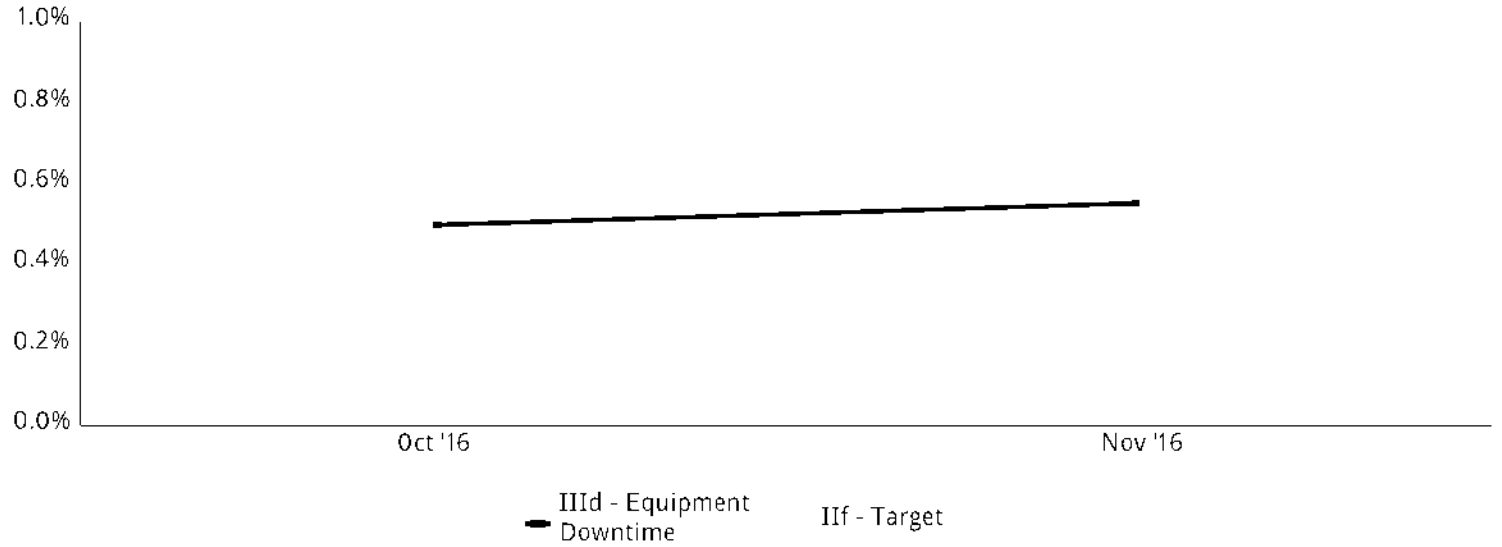
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IIId - Equipment Downtime



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	0.7%	1.0%	148.0%	13.7%
Region 2	0.5%	1.0%	204.7%	17.3%
Region 3	0.4%	1.0%	233.4%	14.3%
Region 4	0.5%	1.0%	217.7%	10.5%
Region 5	0.4%	1.0%	238.6%	10.9%
Region 6	0.6%	1.0%	163.5%	19.6%
Region 7	0.5%	1.0%	189.0%	13.7%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password protected. Electronically transmitted or mailed on password-protected servers.

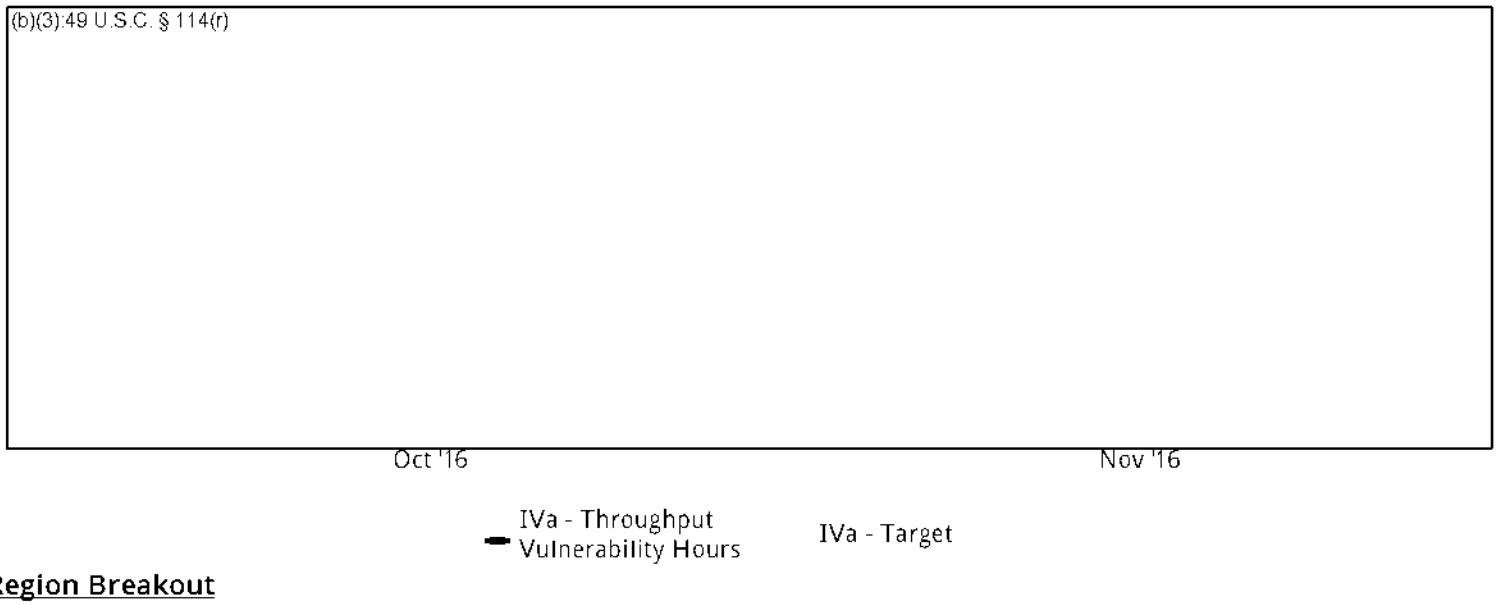
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IVa - Throughput Vulnerability Hours



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-trained on password-protected servers.

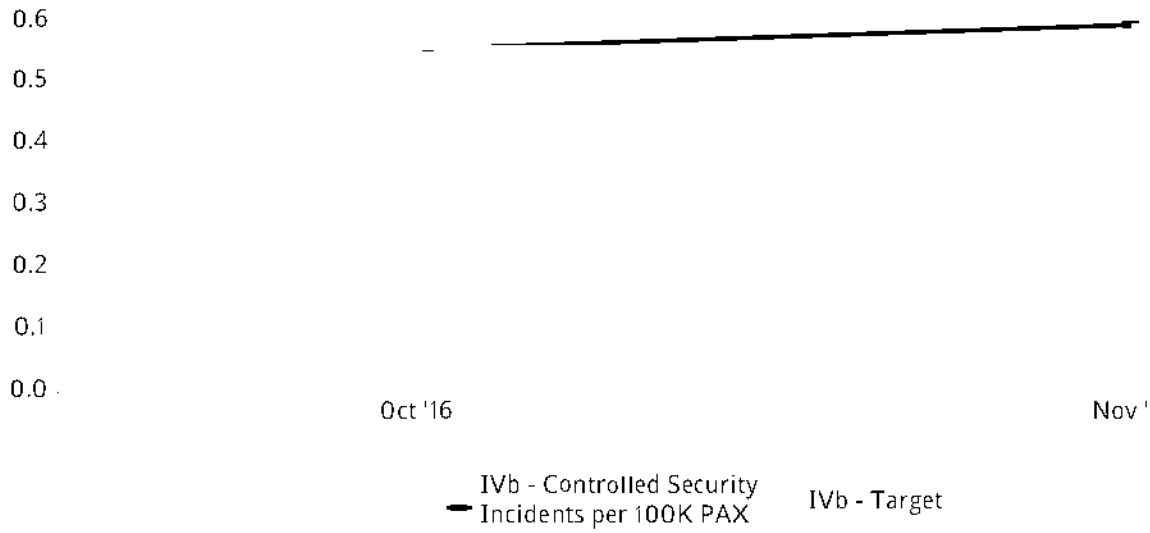
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IVb - Controlled Security Incidents per 100K Pax



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	0.39	0.45	113.8%	14.4%
Region 2	0.48	0.49	103.4%	15.9%
Region 3	0.86	0.82	95.2%	14.7%
Region 4	0.55	0.46	84.5%	10.7%
Region 5	0.90	0.95	105.5%	9.0%
Region 6	0.47	0.46	96.6%	23.1%
Region 7	0.55	0.45	81.7%	12.3%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

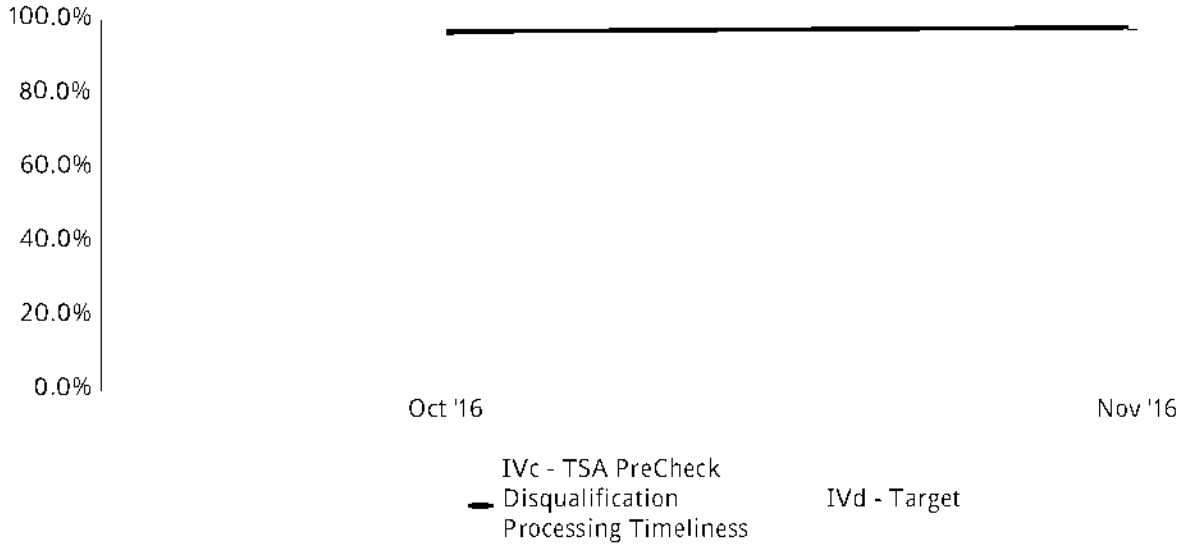
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

November 2016

IVc - PreCheck Disqualification Program Processing Timeliness



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	97.5%	100.0%	97.5%	3.8%
Region 2	98.2%	100.0%	98.2%	15.7%
Region 3	97.3%	100.0%	97.3%	14.7%
Region 4	98.2%	100.0%	98.2%	20.0%
Region 5	98.2%	100.0%	98.2%	17.3%
Region 6	98.0%	100.0%	98.0%	15.4%
Region 7	94.5%	100.0%	94.5%	13.2%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

Transportation Security Administration

U.S. Department of Homeland Security
Office of Security Operations
Arlington, VA 22202

November 8, 2016

From: Benjamin Sears
Branch Manager, Performance Management Branch
Security Operations

To: TSA Leadership

Subject: FY17 Measures of Effectiveness Report – October 2016

Performance Management is pleased to release the October Measures of Effectiveness (MOE) Report. This is the first report for the 2017 fiscal year.

Some key notes on the following metrics:

Ia – National Training Plan (NTP) on Pace: TSIs and STSIs are now included in the NTP file.

Ib – Annual proficiency Review (APR) Variance: This data is representative of CY16 and will be reset in January.

Ic – Annualized FTE including Overtime (excluding managers): NFC has not finalized PPs 20 or 21, and will be added once processed.

Ie – Traumatic Injury Hours: NFC has not finalized PPs 20 or 21 and will be added once processed.

IIb – On Screen Alarm Resolution Protocol (OSARP) (b)(3):49 U.S.C. § L3 data was not included this month due to an issue with the vendor. This data will be reset in January.

IIc – Threat Image Projection (TIP) (b)(3):49 U.S.C. § The TIP remediation percentage was changed to match the latest TIP OD which goes into effect April 1, 2017.

IIIa and IIIb – Mission Essential Level Detect/Deter: The new baseline was created using FY16 data as well as future (2017) AIT deployments.

IIIc – Compliance Finding Resolution: FY to date data has been reset, however is reflective of inspections resulting in a finding in September with follow-up inspections due in October.

IVa – Throughput Vulnerability Hours: The baseline for this metric is FY16 and will not change as FY17 progresses.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.

Please find attached your Nationwide, Region, and Hub-specific MOE.

The first FY17 MOE post-publication call will occur this Thursday, November 10th, 2016, following MOE publication at 14:00. I have included the call details below for all who would like to attend.

Measures of Effectiveness Report Conference Call – October 2016 Publication
Call Line: (b)(6)
Participant Code: (b)(6)

For additional information, Reference Guides, or supporting data see the Performance Management iShare, or contact the MOE Team at MOEHelpDesk@tsa.dhs.gov.

As always, please let us know if you have any questions or need anything else.

~~WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.~~

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
Workforce Readiness Measures that emphasize staffing, training, development, and preparedne required equipment and perform mission-essential functions.				95.5%	30.0
Ia - National Training Plan (NTP) on Pace	93.3%	93.3%	90.0%	100%*	10.0
Ib - Annual Proficiency Review (APR) Variance	12.4%	12.4%	15.0%	100%*	5.0
Ic - Annualized FTE including Overtime (excluding managers)		0.0	44,153.4	100.0%	5.0
Id - Unscheduled Absences	3.4%	3.4%	2.5%		5.0
Ie - Traumatic Injury Hours	0.0	0.0	0.0	100.0%	5.0

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
Workforce Performance Measures that reflect the effectiveness of the workforce in				(b)(3):49 U.S.C. § 114(r)	30.0
IIa - Selectee Find Rate (TSA Miss)**	(b)(3):49 U.S.C. § 114(r)				
IIb - On Screen Alarm Resolution Protocol (OSARP	(b)				
IIc - Threat Image Projection (TIP	(b)				
IId - ASAP Detection Rate					

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
System Readiness Measures that demonstrate that appropri available to perform the mission for whic				(b)(3):49 U.S.C. § 114(r)	20.0
IIIa - Mission Essential Level: Detect	(b)(3):49 U.S.C. § 114(r)				
IIIb - Mission Essential Level: Deter					
IIIc - Compliance Finding Resolution	89.2%	89.2%	100.0%	89.2%	5.0
IIId - Equipment Downtime	0.5%	0.5%	1.0%	100%*	2.5

	Period Actual	FY17 to Date	FY17 Target	% Effective	Weight
System Performance Measures that reflect the overall effectiveness of the system in achieving system detection standards and the desired effects of deter, detect, disrupt.				(b)(3):49 U.S.C. § 114(r)	
IVa - Throughput Vulnerability Hours	(b)(3):49 U.S.C. § 114(r)				
IVb - Controlled Security Incidents per 100K PAX					
IVc - TSA PreCheck Disqualification Processing Timeliness	97.2%	97.2%	100.0%	97.2%	7.5

Overall Effectiveness

96.7%

* This metric's % effective has been capped at 100%
** This metric's target may change if an airport has <200 selectees

Default Color Coding (except for Ic and IIa): 85% - 95% >95%

Please see the MOE Reference Guide for additional metric-specific information

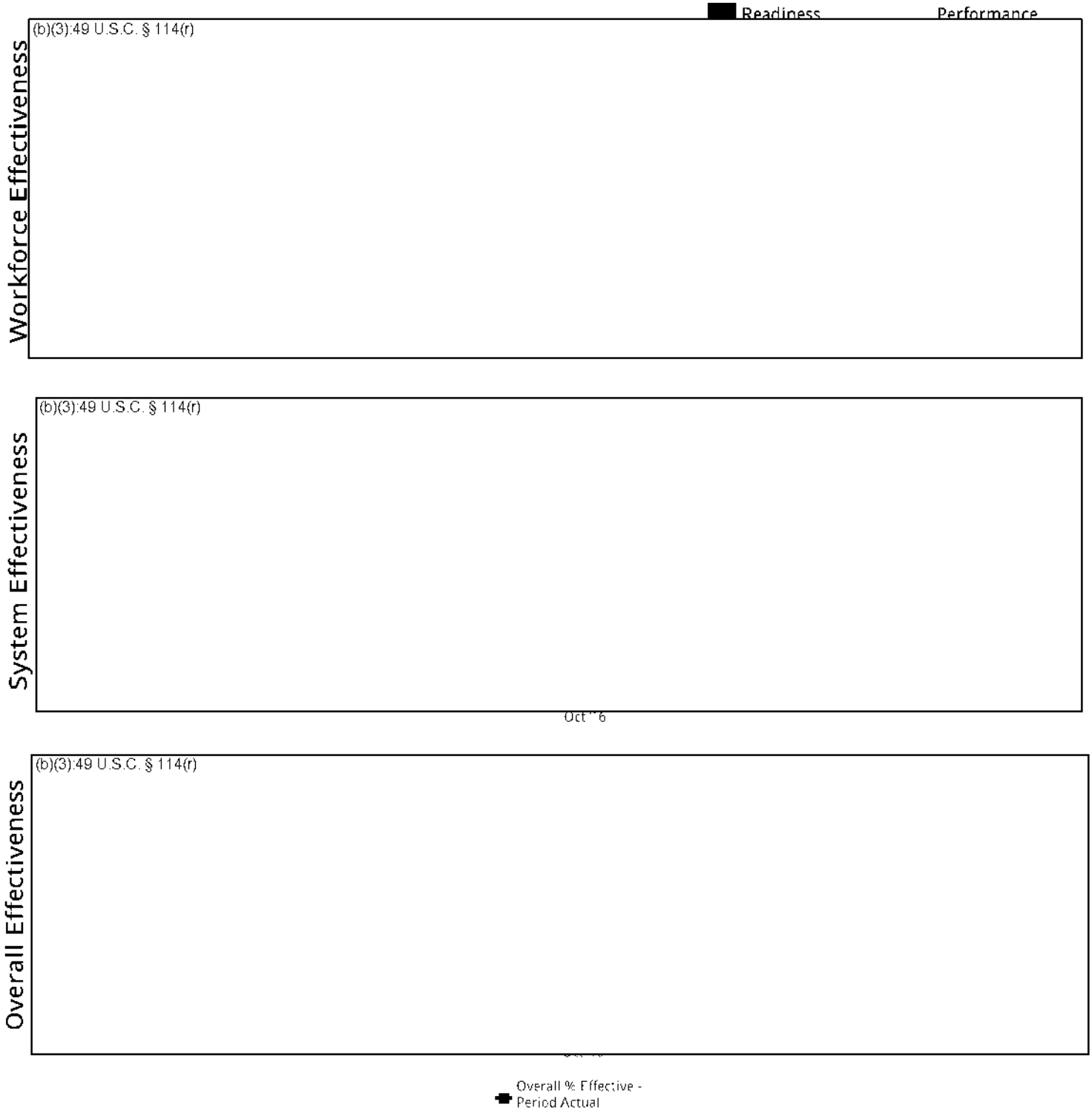
(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-tained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016



(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

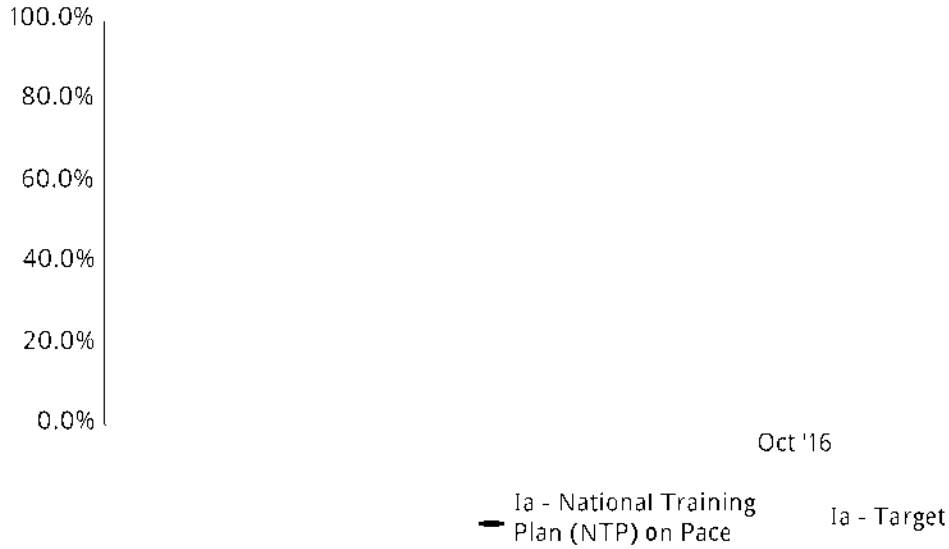
FY17 Measures of Effectiveness

Nationwide

October 2016

Ia - National Training Plan (NTP) on Pace

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	94.0%	90.0%	104.5%	14.7%
Region 2	92.2%	90.0%	102.5%	16.3%
Region 3	93.3%	90.0%	103.7%	15.3%
Region 4	93.9%	90.0%	104.3%	10.8%
Region 5	92.9%	90.0%	103.3%	9.4%
Region 6	93.8%	90.0%	104.3%	20.9%
Region 7	93.0%	90.0%	103.4%	12.6%

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.~~

TRANSPORTATION SECURITY ADMINISTRATION

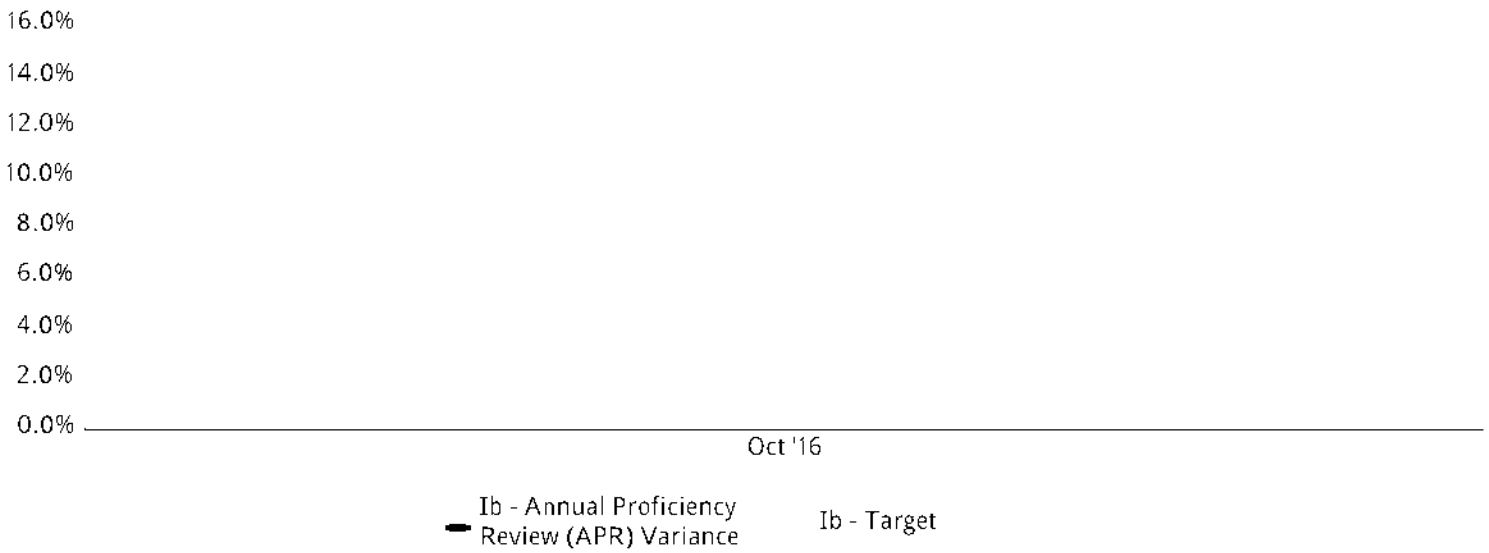
FY17 Measures of Effectiveness

Nationwide

October 2016

Ib- Annual Proficiency Review (APR) Variance

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	13.8%	15.0%	108.7%	14.2%
Region 2	11.8%	15.0%	127.4%	16.5%
Region 3	11.7%	15.0%	128.1%	15.8%
Region 4	11.1%	15.0%	134.8%	11.2%
Region 5	11.6%	15.0%	129.0%	9.1%
Region 6	12.2%	15.0%	123.0%	20.7%
Region 7	14.5%	15.0%	103.7%	12.5%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

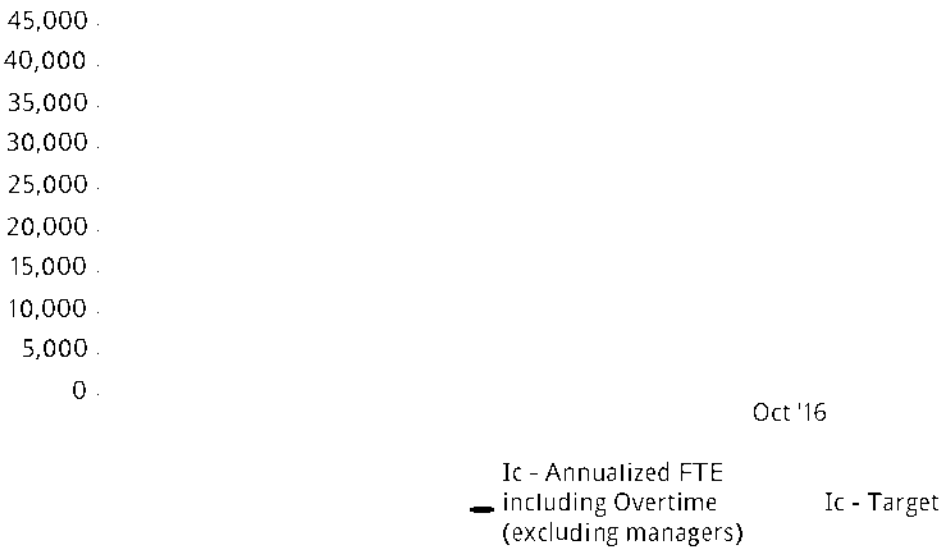
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

Ic- Annualized FTE including Overtime (excluding managers)



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1		6,588.7	100.0%	
Region 2		7,239.7	100.0%	
Region 3		6,600.3	100.0%	
Region 4		4,898.4	100.0%	
Region 5		4,384.8	100.0%	
Region 6		8,699.5	100.0%	
Region 7		5,742.1	100.0%	

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or retrieved on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

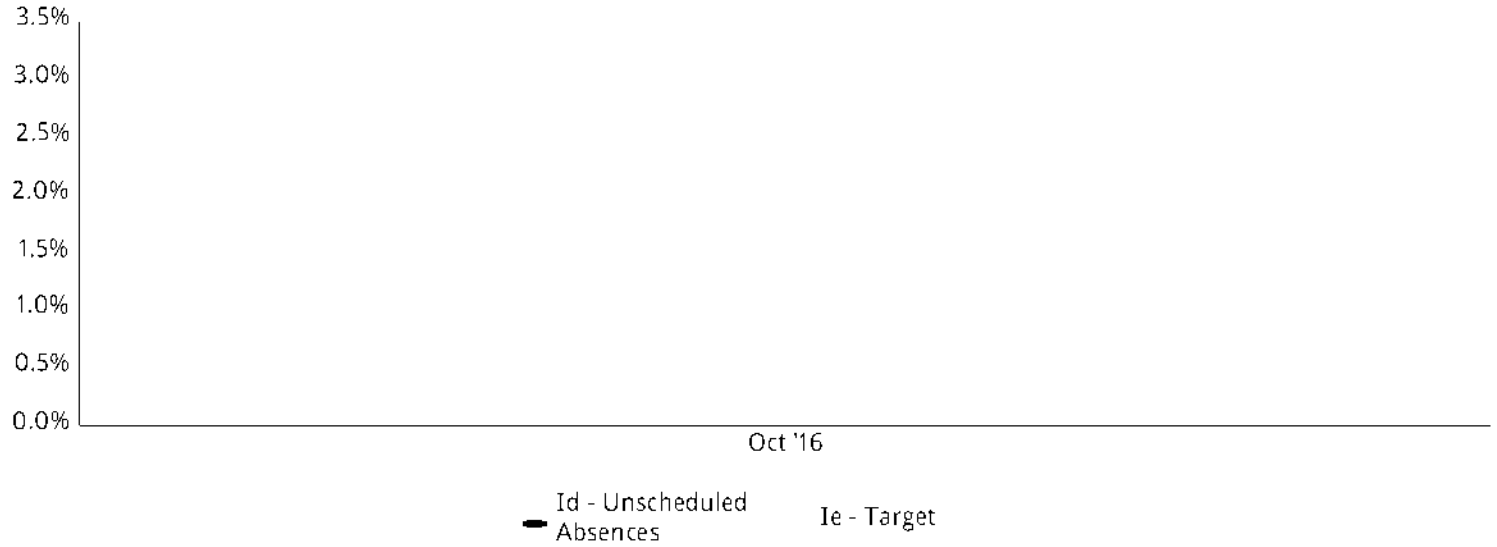
FY17 Measures of Effectiveness

Nationwide

October 2016

Id- Unscheduled Absences

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	4.3%	3.1%	71.8%	14.9%
Region 2	4.0%	2.6%	64.8%	15.1%
Region 3	3.1%	2.4%	77.0%	15.8%
Region 4	3.3%	2.4%	72.4%	11.2%
Region 5	3.0%	2.2%	72.0%	9.4%
Region 6	2.9%	2.3%	80.5%	21.5%
Region 7	3.4%	2.4%	72.4%	12.1%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

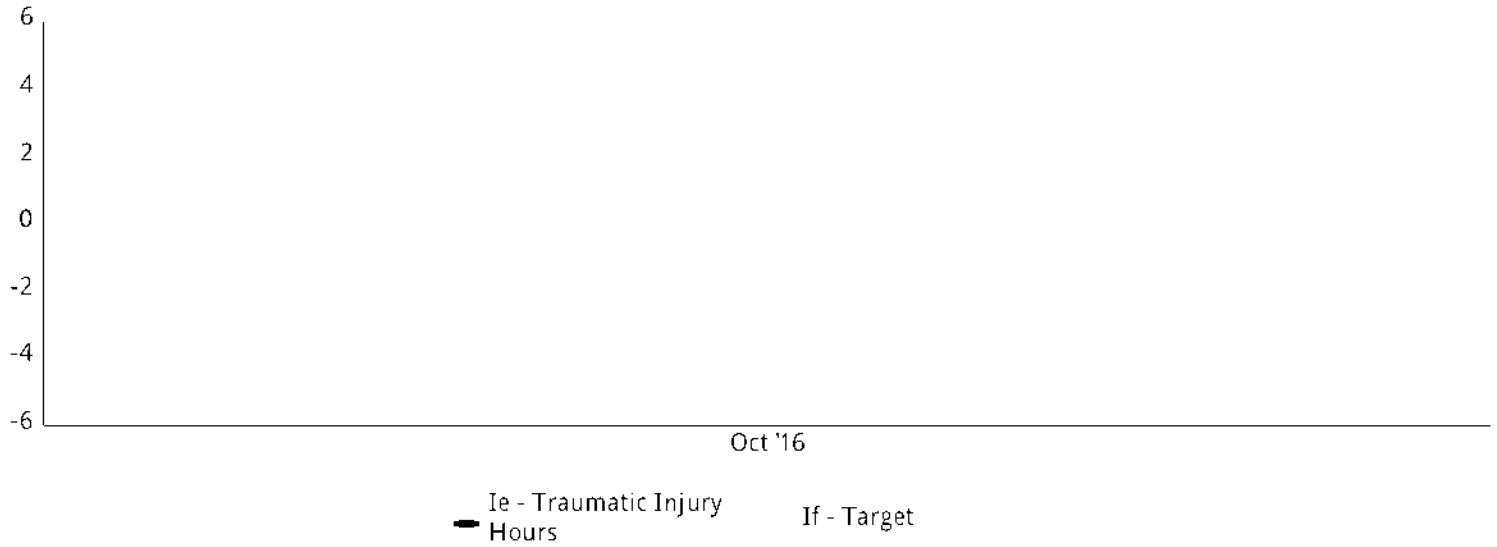
FY17 Measures of Effectiveness

Nationwide

October 2016

Ie- Traumatic Injury Hours

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	0.0	0.0	100.0%	
Region 2	0.0	0.0	100.0%	
Region 3	0.0	0.0	100.0%	
Region 4	0.0	0.0	100.0%	
Region 5	0.0	0.0	100.0%	
Region 6	0.0	0.0	100.0%	
Region 7	0.0	0.0	100.0%	

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-gained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

IIa - Selectee Find Rate (TSA Miss)

[redacted]

(b)(3):49 U.S.C. § 114(r)

Oct '16

IIa - Selectee Find Rate (TSA Miss)**

IIIa - Target

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed on password-protected servers.~~

TRANSPORTATION SECURITY ADMINISTRATION

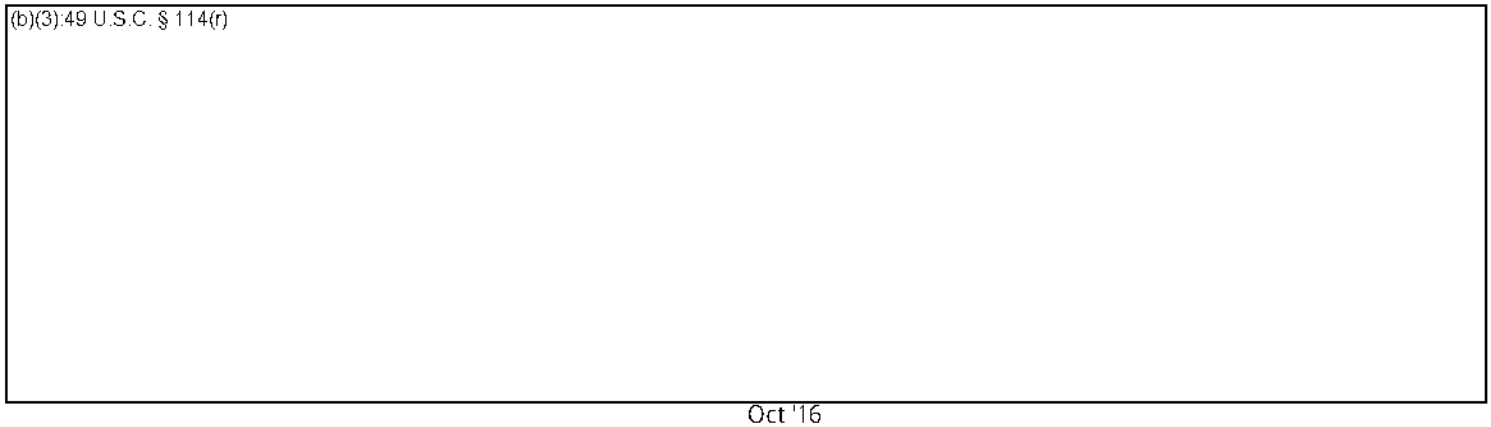
FY17 Measures of Effectiveness

Nationwide

October 2016

IIb - On Screen Alarm Resolution Protocol (OSARP) (b)(3):49 U.S.C. § 1 [redacted]

(b)(3):49 U.S.C. § 114(r)



Oct '16

IIb - On Screen Alarm Resolution Protocol (OSARP) (b)(3):

IIIb - Target

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed files on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

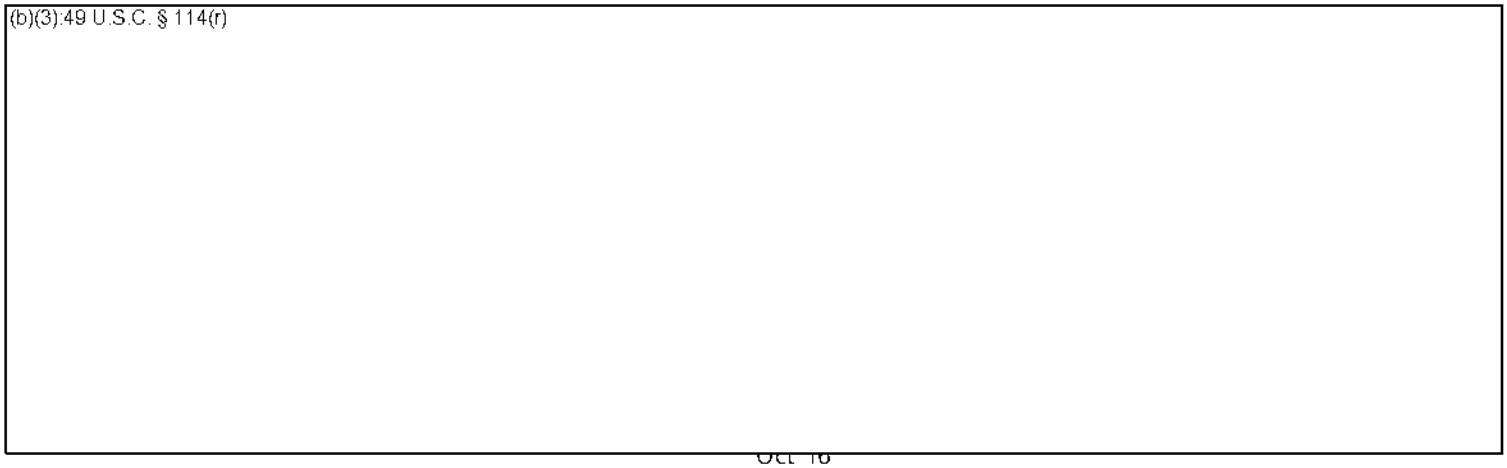
FY17 Measures of Effectiveness

Nationwide

October 2016

IIc - Threat Image Projection (TIP) (b)(3):49 U.S.C. §

[redacted]



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

~~(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.~~

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

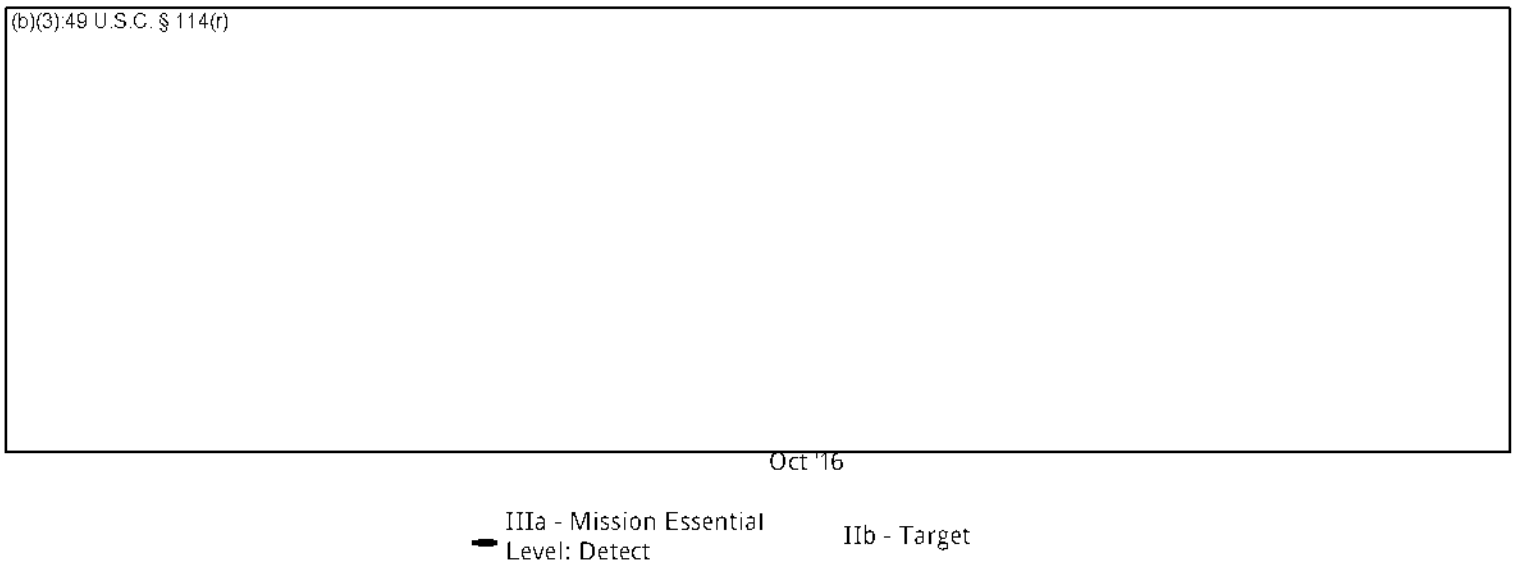
Nationwide

October 2016

IIIa - Mission Essential Level: Detect

[redacted]

(b)(3):49 U.S.C. § 114(r)



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

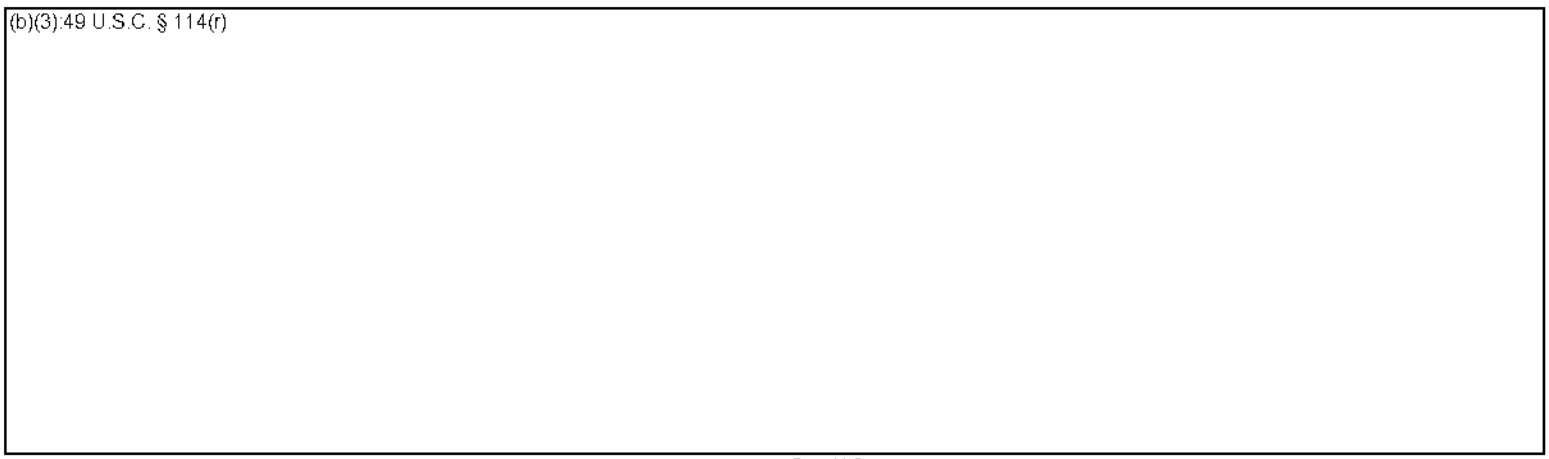
Nationwide

October 2016

IIIb - Mission Essential Level: Deter

[redacted]

(b)(3):49 U.S.C. § 114(r)



Oct '16

IIIb - Mission Essential Level: Deter

IIc - Target

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

IIIc - Compliance Finding Resolution

[redacted]

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	93.2%	100.0%	93.2%	17.4%
Region 2	93.7%	100.0%	93.7%	34.5%
Region 3	83.0%	100.0%	83.0%	10.5%
Region 4	85.7%	100.0%	85.7%	11.0%
Region 5	92.2%	100.0%	92.2%	10.1%
Region 6	80.0%	100.0%	80.0%	9.9%
Region 7	79.4%	100.0%	79.4%	6.7%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

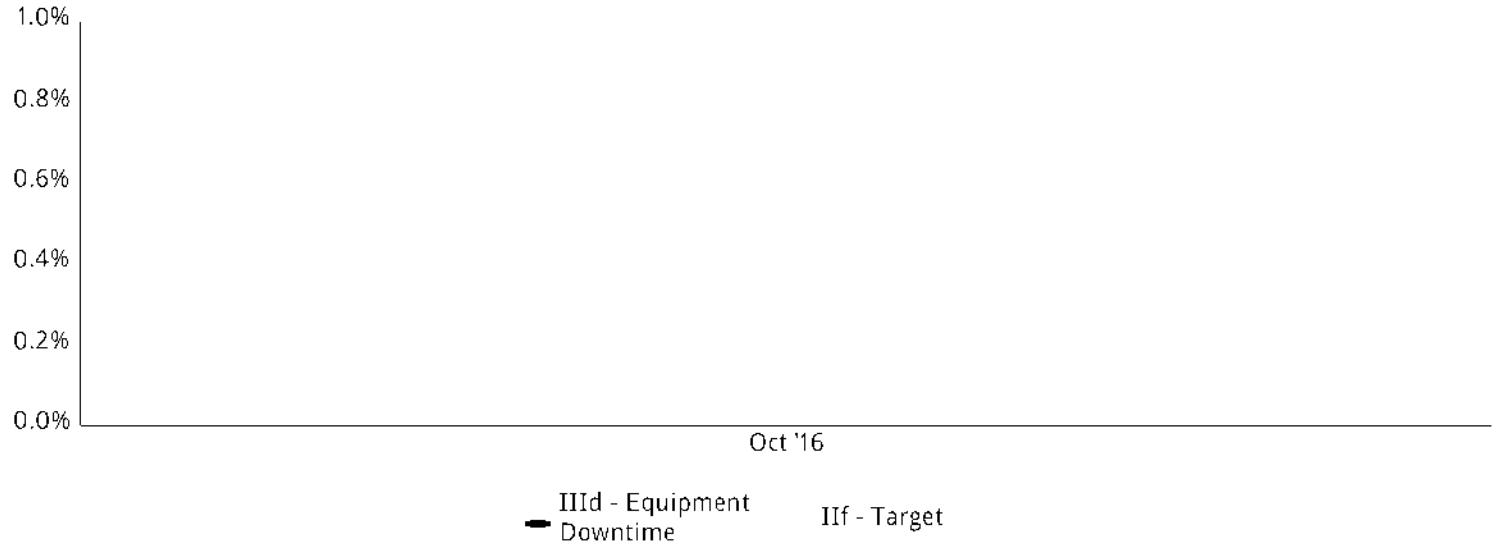
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

IIId - Equipment Downtime



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	0.6%	1.0%	167.6%	13.7%
Region 2	0.5%	1.0%	214.3%	17.3%
Region 3	0.3%	1.0%	302.1%	14.3%
Region 4	0.4%	1.0%	234.0%	10.4%
Region 5	0.5%	1.0%	214.7%	10.9%
Region 6	0.5%	1.0%	183.5%	19.6%
Region 7	0.6%	1.0%	161.5%	13.7%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mail-farmed on password-protected servers.

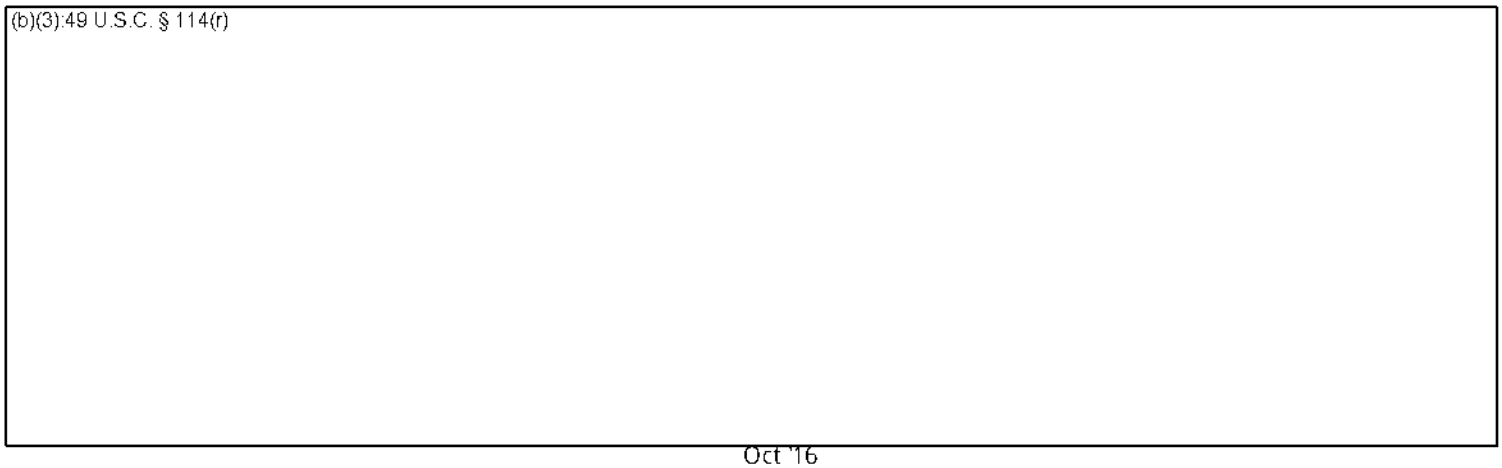
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

IVa - Throughput Vulnerability Hours



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	(b)(3):49 U.S.C. § 114(r)			
Region 2				
Region 3				
Region 4				
Region 5				
Region 6				
Region 7				

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or mailed on password-protected servers.

TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

IVb - Controlled Security Incidents per 100K Pax

Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	0.44	0.45	102.8%	14.6%
Region 2	0.46	0.49	106.9%	15.1%
Region 3	0.82	0.82	100.3%	14.9%
Region 4	0.51	0.46	91.0%	10.6%
Region 5	0.75	0.95	127.2%	9.1%
Region 6	0.46	0.46	99.9%	23.2%
Region 7	0.60	0.45	75.6%	12.5%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

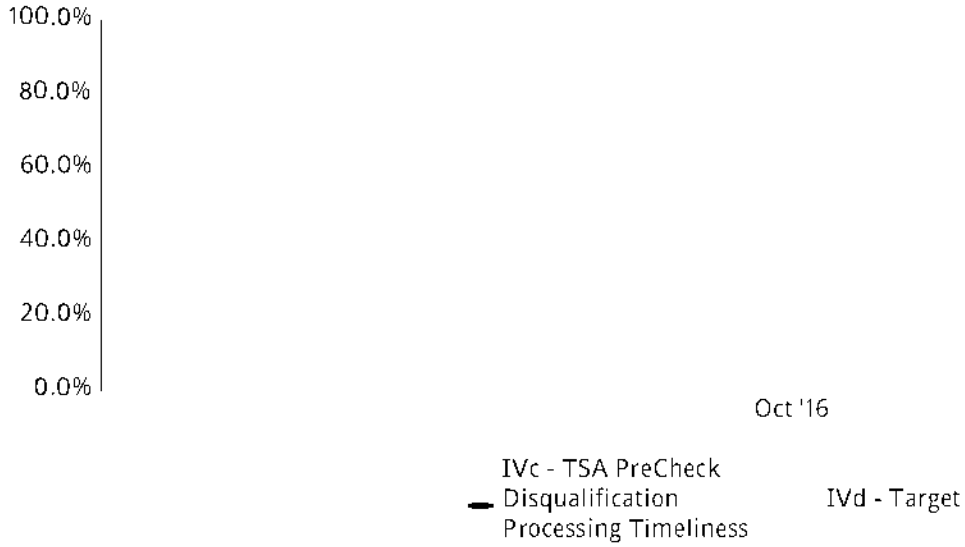
TRANSPORTATION SECURITY ADMINISTRATION

FY17 Measures of Effectiveness

Nationwide

October 2016

IVc - PreCheck Disqualification Program Processing Timeliness



Region Breakout

Region	FY17 to Date	FY17 Target	% Effective	Contribution to Nation
Region 1	95.8%	100.0%	95.8%	3.4%
Region 2	98.5%	100.0%	98.5%	15.7%
Region 3	96.6%	100.0%	96.6%	15.8%
Region 4	98.5%	100.0%	98.5%	19.4%
Region 5	98.1%	100.0%	98.1%	18.0%
Region 6	96.9%	100.0%	96.9%	14.2%
Region 7	94.3%	100.0%	94.3%	13.6%

(U) WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. Note: This document must be password-protected. Electronically transmitted or maintained on password-protected servers.

Transportation Security Administration

Transportation Security Officer at DCA using advanced imaging technology to safely screen passengers for metallic and nonmetallic threats, including weapons and explosives, which may be concealed under clothing, without physical contact.

The Transportation Security Administration (TSA) was created in 2001 by the enactment of the *Aviation and Transportation Security Act of 2001* in the aftermath of the September 11, 2001 terrorist attacks. TSA's nearly 60,000 employees are charged with protecting U.S. transportation systems and the traveling public.

Immediately following its creation, TSA implemented numerous security programs, standards, and protocols, which continue to be refined and updated based on a continuous assessment of threats and risks. These include:

- Passenger and baggage screening through explosives detection systems and utilizing canine teams. Fortifying aircraft cockpit doors
- Implementing the Federal Flight Deck Officer program to train flight-deck personnel to carry firearms,
- Deploying Federal Air Marshals on high-risk domestic and international flights
- Establishing Visible Intermodal Prevention and Response (VIPR) teams to provide a visible and flexible deterrent in all modes of transportation.
- Implementing the Secure Flight program to vet all passengers on flights within the U.S. and inbound to or outbound from the - U.S. against watch lists

Canine Officer in Miami, Florida. TSA's explosives detection canines are trained on a variety of explosives based on intelligence data and emerging threats. Photo by Brigitte Dittberner

~~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.~~

In addition to its well-known role providing aviation security, TSA is responsible for security in all surface modes of transportation. The Nation's surface transportation systems affect the daily life of many Americans and are critical to the economy and security of the United States.

More than 500 individual freight railroads operate on nearly 140,000 miles of track carrying essential goods. Eight million large capacity commercial trucks and almost 4,000 commercial bus companies travel on the four million miles of roadway in the United. Surface transportation operators carry approximately 750 million intercity bus passengers and 10 billion passenger trips on mass transit each year. The pipeline industry consists of approximately 3,000 private companies who own and operate more than 2.5 million miles of pipelines transporting natural gas, refined petroleum products, and other commercial products.

Average TSA Day

Aviation Security

- TSA screens approximately 2 million passengers daily
- TSA screens 1.3 million checked items for explosives and other dangerous items daily
- TSA screens 4.9 million carry-on items for explosives and other prohibited items every day
- Signs up over 10,000 passengers for TSA Pre✓® at more than 385 locations nationwide
- Recurrently vets over 16 million persons with access to the transportation system for ties to terrorism

Federal Air Marshals are highly trained professionals dedicated to ensuring transportation security. Photo by Transportation Security Administration

- Responsible for the security of over 20,000 domestic flights per day
- Responsible for the security of over 2,000 outbound international flights per day
- Approximately seven firearms are found at the screening checkpoints per day

Inbound International Aviation

- TSA teams of security professionals are assessing foreign airports around the world, including approximately 260 Last Point of Departure airports and FAA certified foreign repair stations, to determine if they are meeting international security requirements, and are also inspecting air carriers to determine if they adhere to U.S. security programs.
- TSA Representatives (TSAR) stationed at strategic locations around the world are coordinating with their foreign government counterparts to ensure the security of inbound flights to the U.S.

Law Enforcement

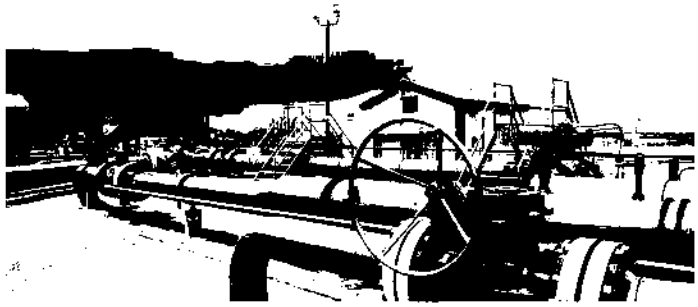
- Federal air marshals fly thousands of miles each day
- More than 900 explosive detection canine teams trained and deployed nationwide, tasked with screening passengers and cargo, and supporting other security missions

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.

- TSA performs 24 Visible Intermodal Prevention and Response (VIPR) operations at airports, and other transportation facilities each day.

Multi-modal Security Efforts

- More than 246 compliance inspections are conducted daily across all modes in support of risk-based security
- Approximately 8 billion trips were taken on public transportation
- TSA vets more than 15 million holders of transportation credentials against watch lists.
- TSA collaborates with transit agencies to provide for the security of the 27 million passenger trips occurring daily in our nation's mass transit systems



TSA's Surface Pipeline Security Branch is responsible for working with private entities to enhance security preparedness of 2.6 million miles of national hazardous liquid and natural gas pipeline systems. Photo by Transportation Security Administration

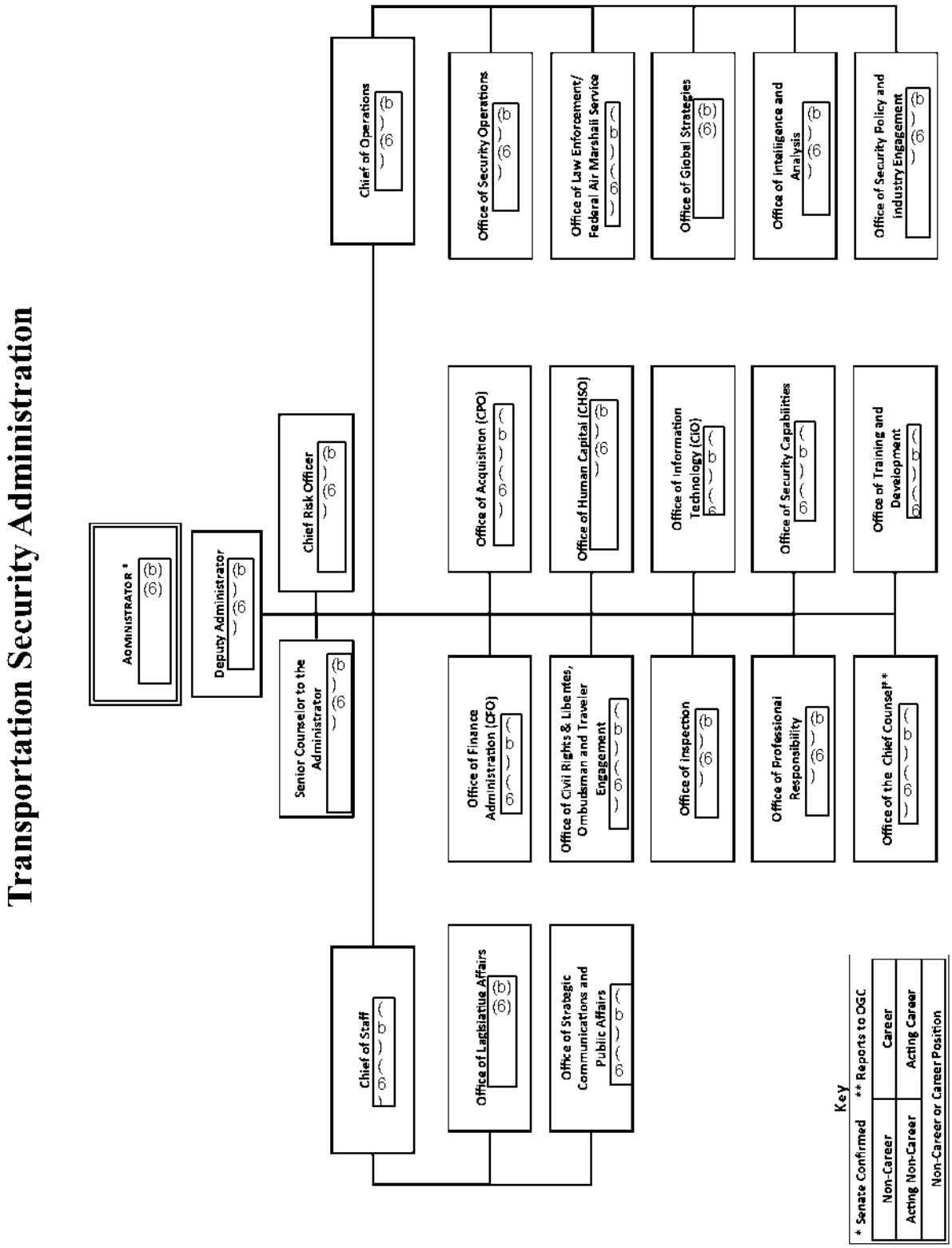
- More than 27 million passenger trips occur on mass transit systems that TSA collaborates with to ensure the security of passengers

Mission

Protect the nation's transportation systems to ensure freedom of movement and commerce.

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.

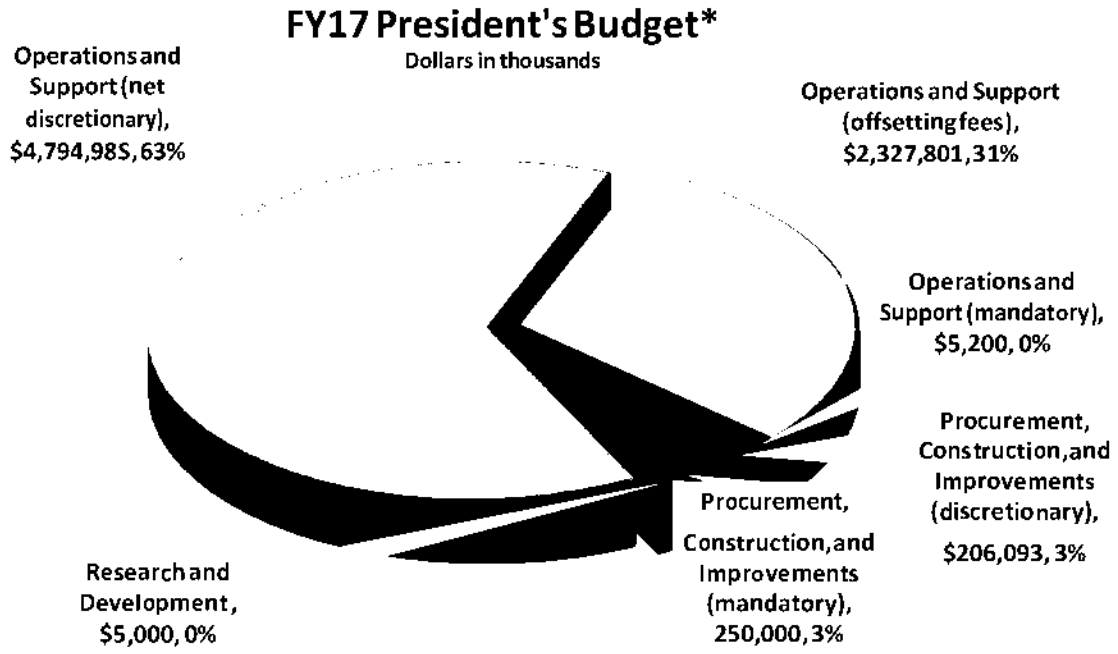
Organization Chart



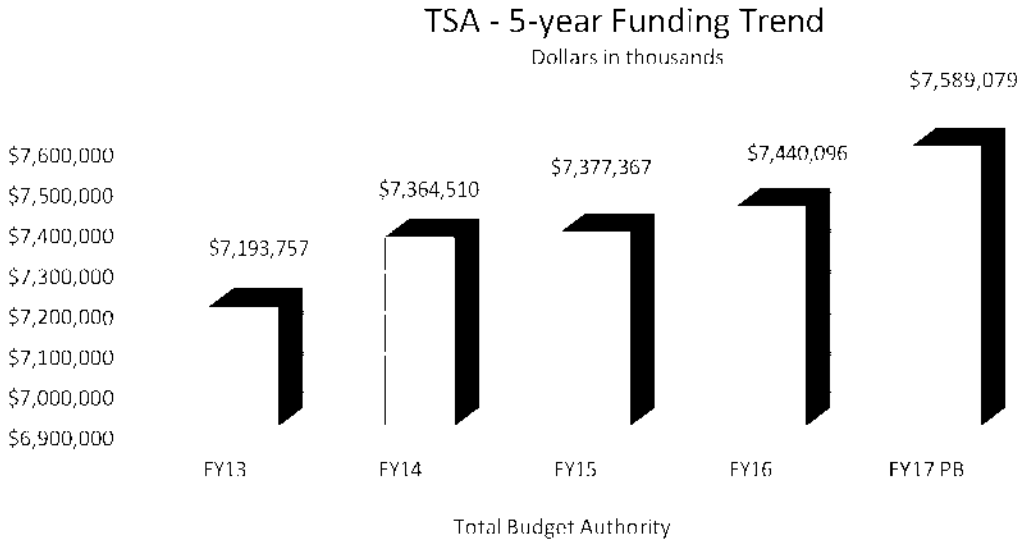
Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, 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

TSA - Total Budget Authority		
$7,440,096,000	$7,589,079,000	$148,983,000



*Does not include a $171.633K impact on FY17 from FY16 reprogramming.

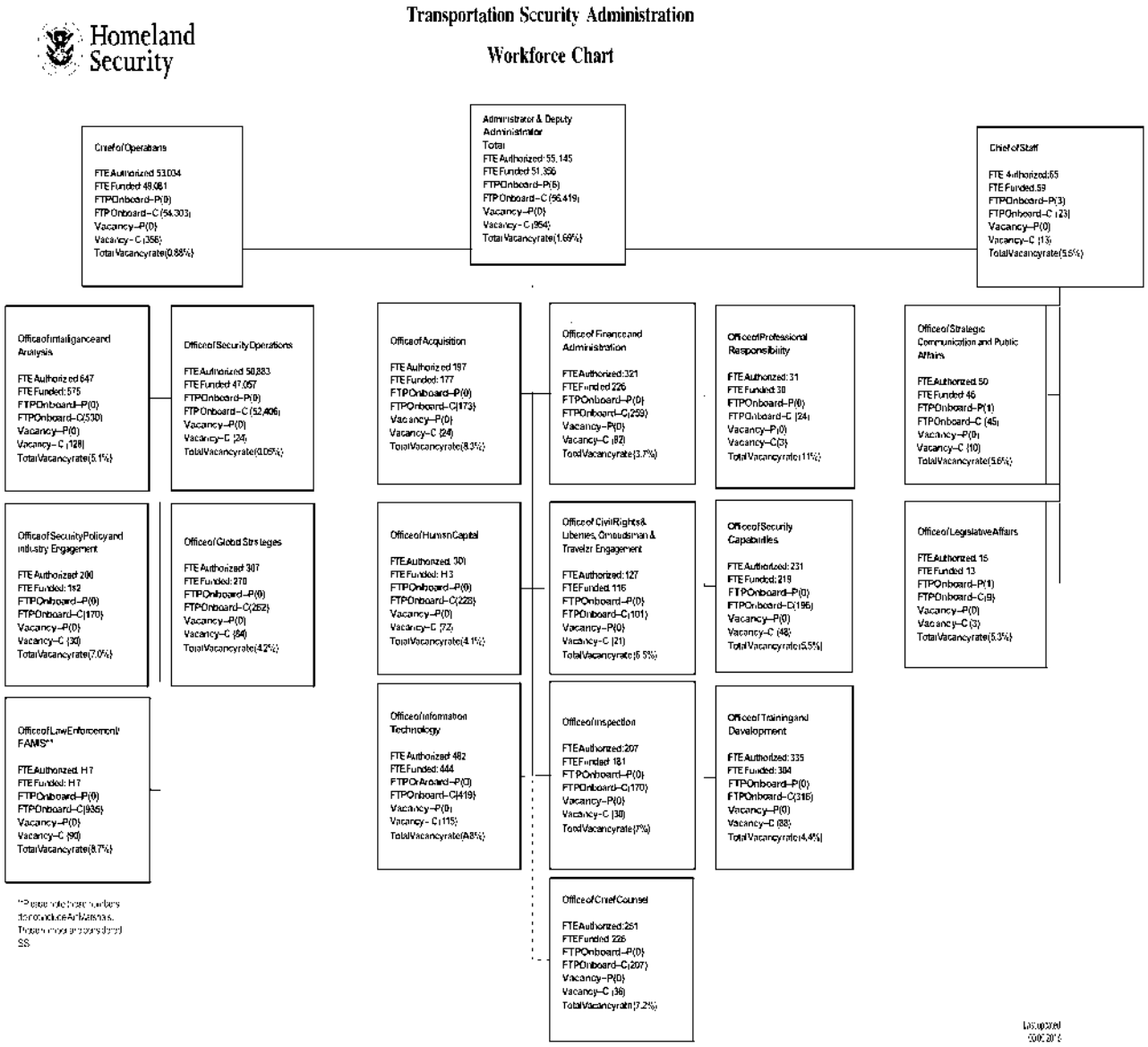


~~Warning! This document, along with any attachments, contains NON-PUBLIC INFORMATION exempt from release to the public by federal law. It may contain confidential, legally privileged, proprietary or deliberative process inter-agency/intra-agency material. You are hereby notified that any dissemination, 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.~~

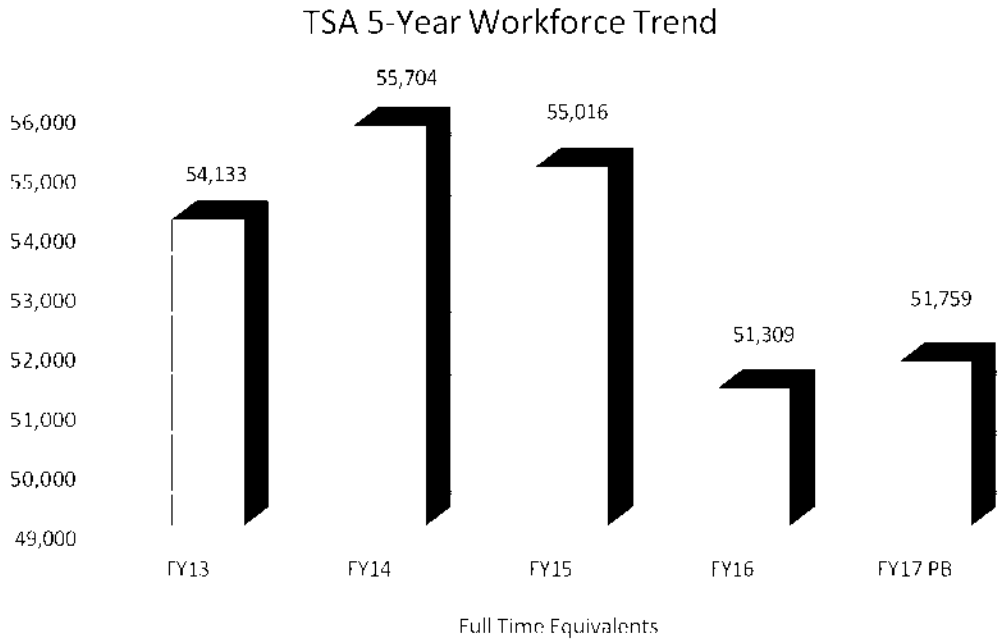
Workforce

55,145	56,419**	954

* FY 2016. Does not include reimbursable, working capital, or revolving account employees
**Onboard number reflects full- and part-time personnel



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

- Rebalance and Invest in the Workforce - Passenger volume growth increased 5% in FY15 and is estimated to increase 6.5% for FY16. Working with airline stakeholders, reviewing Federal Aviation Administration forecasted growth, and analyzing the Bureau of Transportation Statistics historical enplanement data, TSA is currently forecasting passenger volume to increase by 4% in FY17, by 3% in FY18, and then to normalize increased passenger volumes at 2.5% for subsequent years. The demand and ridership for mass transit systems in urban and high population density areas increased by 22% since 1990. Most of these systems operate at near capacity levels and increases in capacity are constrained by high cost of expansion. Since they operate close to capacity levels, any disruption can have significant impact on the local economy.

More than 60 percent of TSA officers have five years or more experience as counterterrorism professionals. Photo by Transportation Security Administration

In Fiscal Year (FY) 2015, TSA's frontline staffing levels reached their lowest point in five years. TSA evaluated total workforce requirements and identified several areas requiring additional support in order to build a professional, highly trained counterterrorism workforce with the right people in the right places at the right time. These areas include staffing for volume increases, improving hiring screening processes, enhancing the full time to part time ratio to 90% full time, improving the ratio of supervisors in place at the largest airports, enhancing the

~~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.~~

professionalization of the workforce through fully funding training hours and annual and sick leave liability, additional TSA Pre✓® lane coverage across the nation's airports, and increased canine teams. TSA is also building out a new TSA Academy Center of Excellence training facility at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA, to provide initial and recurrent training for the TSA screening workforce, requiring additional mission-focused training for Senior Executives, and expanding its leadership and professional development program for all employees.

- Enterprise-wide Human Resources (HR), Acquisition, and Planning, Programing, Budget and Execution Reform -
    - TSA is implementing a strategic approach to HR management. The first phase of the approach is to increase in-house services by assessing inherently governmental functions and those best served by multiple contract vendors, then transitioning away from the current single vendor contract. The second phase is to move from the current decentralized control of HR functions to a centralized system to manage human capital and employee/labor relations.

    - TSA is also reforming its acquisition program to improve its cost-benefit analyses, performance measurements, integrated master schedule development and maintenance, relationship with the DHS Science and Technology Directorate, and program baseline establishment/management. TSA is taking the following actions to achieve its acquisition reform goals:
        - Establish a Capabilities and Requirements Office reporting to the Chief of Operations;
        - Realign the Operational Test Agent from the Office of Security Capabilities to the Chief of Operations;
        - Appoint the Deputy Administrator as the Component Acquisition Executive and align the acquisition program management function to the Office of Acquisition, who will serve as the Deputy Component Acquisition Executive; and
        - Create of an independent Office of Contracts and Procurement.

Transportation security officers screen approximately 2 million passengers each day at approximately 440 airports nationwide. Officers are trained to spot prohibited items, and on average, discover seven firearms per day at security checkpoints. Photo by Vivien Lau

    - TSA is working to strengthen the linkages between strategy, budget, execution, and performance through a comprehensive Planning, Programming, Budget, and Execution (PPBE) resource management system led by an analytic programming branch in fall 2016 for the FY19 budget development. TSA is also working with DHS to provide detailed PPBE training to all key personnel within the resource management offices.

- Intel-driven Operations - TSA is focusing on enhancing intelligence and counter-intelligence capabilities, information sharing, and frontline employee communications to identify and

~~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.~~

disseminate intelligence indicators and patterns that could point to potential terrorist plots or attacks against transportation. TSA is also enhancing its security threat assessment processes by implementing intergovernmental partnerships that will add the capability to continuously vet against criminal information databases, and improve TSA's ability to vet the more than 16 million transportation workers and 700 million passengers annually.

- Federal Air Marshal Service Hiring and Retention and Visible Intermodal Prevention and Response expansion -
    - TSA will continue hiring Federal Air Marshal Service (FAMS) personnel to meet key operational requirements to include both international and domestic coverage goals, as well as better effectiveness to redirect mission flight resources, when required. FAM hiring will also allow for improved FAMS diversity, workforce morale, and agency sustainability.
    - TSA continues to increase the efficiency and effectiveness of the VIPR program through active engagement with counterpart law enforcement and aviation-focused organizations and the implementation of the VIPR CONOPS to further integrate a risk based approach for prioritizing and scheduling VIPR operations. Current congressional legislation provides for the addition of 6 VIPR Teams to continue to strengthen the risk-based approach to deploy integrated TSA assets using law enforcement and screening capabilities in coordinated activities to augment the security of any mode of transportation.

The Federal Air Marshal Service has the highest qualification standards for marksmanship in the federal law enforcement community. Photo by Transportation Security Administration

- Last Point of Departure and Overseas Focus as Threat Increases - The threat to commercial aviation remains a predominant focus of terrorists and extremists based on intelligence reporting and recent terrorist actions that have been executed to include the attack on the Brussels Airport. TSA is continuing to assess 280 airports in approximately 100 countries with Last Point of Departure (LPD) service to the United States, and uses a Foreign Airport Assessment Program to identify existing and potential vulnerabilities at the specified airports as well as those serviced by U.S. aircraft operators. In addition, the Federal Air Marshals Service (FAMS) continues to focus on high threat LPDs, and adjusts schedules to respond to Known or Suspected Terrorist (KST) travel on US carriers. TSA is also continuing to focus on carrier/aircraft crewmember vetting and issue Security Directives and Emergency Amendments to U.S. aircraft operators and foreign air carriers to raise security standards and mitigate threats and vulnerabilities.

~~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**
Department of Transportation (DOT)	TSA, along with DOT and the U.S. Coast Guard, are Co-Sector Specific Agencies (Co-SSAs) for the Transportation Systems Sector, one of 16 critical infrastructure sectors as identified by the National Infrastructure Protection Plan. As Co-SAAs, the agencies share responsibility to coordinate sector efforts for security preparedness and resilience. Additionally, TSA works with the mode-specific DOT offices on security and safety rulemaking efforts, security and safety standards and guidance documents, and the review of security grant applications to ensure the work TSA and DOT undertake are complementary, do not duplicate work, and do not place an undue burden on transportation systems.
Interagency Airspace Protection Working Group, Department of Transportation (Federal Aviation Administration)	Discuss and work through airspace issues related to the National Capital Region and TSA-regulated parties.

Stakeholder Groups and Federal Advisory Committees (FACA)	
Partner	**Description**
Aviation Security Advisory Committee (ASAC)	Established in 1989 after a terrorist attack on Pan Am flight 103, the ASAC provides advice to the TSA Administrator on aviation security matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security. ASAC is composed of individual members representing private sector organizations affected by aviation security requirements. The Aviation Security Stakeholder Participation Act of 2014, enacted on December 18, 2014, makes the committee permanent. It typically meets four times a year and holds a meeting open to the public once a year.

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.

Industry / Public-Private / Academia	
Partner Name	**Description**
Association of American Railroads, American Short Line and Regional Railroad Association	Key partners in the railroad industry for information sharing, research, development and promulgation of strong security best practices, resources, and programs for all railroads.
American Bus Association, United Motorcoach Association, Trailways Consortium, State and Regional Motorcoach associations	Key partners in the commercial bus industry for research, development, and promulgation of strong security best practices, resources, and programs in the community of passenger motor carriers
Transit Policing and Security Peer Advisory Group (PAG)	Comprised of the top law enforcement and security officials from 26 mass transit and passenger rail and law enforcement agencies across the U.S., Canada, and the United Kingdom, TSA works with the PAG to reduce the risk of terrorism and intentional harm to industry assets, passengers, and employees, and identify funding, equipment, and other resources to achieve that end. Act as a liaison between the industry and the Federal government through conference calls and meetings with the TSA Administrator.
General and commercial aviation industry partners, including air cargo, and all US Commercial Airlines and Federalized Airports	Aviation (commercial and general), airport, and air cargo industry partners, and regulated parties that are critical for communication, collaboration, and information sharing with stakeholders, and implementing security measures mandated by regulations to ensure the safety and security of the airports and aviation modes (commercial, general, and cargo).
American Public Transportation Association	Work to develop security standards on topics such as physical security, cybersecurity, security operations, security planning, and security programs. Facilitate funding for the Information Sharing and Analysis Centers (ISACs), which provides TSA security partners with 24/7 "all threat" warning and incident reporting, early warning, threat identification, and security incident analysis.

~~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.~~

International Engagements	
Partner	**Description**
International Civil Aviation Organization	The International Civil Aviation Organization (ICAO) is a United Nations specialized agency dedicated to enhancing the safety and security of international civil aviation through the development of global standards. TSA is the lead U.S. government agency on matters of aviation security within ICAO and represents the United States on the Aviation Security Panel of Experts and in its various working groups.
The International Air Transport Association	International aircraft operator industry partner for international communications and information sharing

~~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.

Legislative Priorities

- Reauthorization - The authorities contained in TSA's primary authorizing statute, the Aviation and Transportation Security Act (Public Law 107-71), do not require regular reauthorization. As such, legislation pertaining to TSA tends to be narrow in scope and often addresses recommendations of the DHS Inspector General or the Government Accountability Office. The last large-scale TSA reform legislation occurred during the 111th Congress, in 2009. The House passed a TSA reform measure, but the Senate did not consider the measure.

- FY 2016 Reprograming and FY 2017 Fiscal Impact - In the summer of 2016, and in the aftermath of the testing results and the TSA Tiger Team work on checkpoint operations, TSA worked with DHS and Congress to recast the FY 2016 budget request to stabilize the screener workforce. The main objective was to halt a further reduction of over 1,600 screeners. Furthermore, TSA implemented a three point plan of improving checkpoint performance, mitigating passenger volume and mitigating vulnerabilities in security equipment for the balance of FY 2016 to ensure the safety of the traveling public. These stopgap measures improved screening performance, but did not address the 6+% growth of passenger volume observed and projected to continue in 2016 and beyond. Congress approved two FY 2016 reprogrammings of $62M for additional screener overtime, accelerated hiring of 1368 screeners, and conversion of 2,784 part time employees to full time employees. An additional FY 2016 reprogramming of $56M provided funding to purchase replacement explosive trace detection equipment, purchase 80 canines, deploy AIT systems to small and medium sized airports, and accelerate vetting platform enhancements. Since the impact of the FY 2016 reprogrammings were not accounted for in the FY 2017 President's Budget submission, TSA and DHS will continue to work with Congress to address the impacts for FY 2017.

- Passenger Security Fees - The FY 2017 Budget proposes increasing the Aviation Security Fees to collect an additional $908.8 million in FY 2017. Proposed legislation was provided to Congress to raise the passenger fee by one dollar, from $5.60 to $6.60 per one way trip, generating $488.8 million in new revenue. In addition, proposed legislation was provided to Congress to reinstate $420 million in contributions from air carriers, which was the agreed upon amount of security costs paid by the airlines prior to the assumption of these duties by the TSA. This will continue to be a priority for TSA.

- Congressional Engagement - TSA's Office of Legislative Affairs (OLA) informs Members of Congress and staff of TSA accomplishments and shares positive workforce stories with congressional offices representing outstanding employees. These engagements resulted in Member recognition of workforce accomplishments through letters, floor statements, and office visits. OLA, in partnership with the Office of Security Operations, also conducts regular outreach briefings and airport tours for congressional staffers to educate them on TSA operations and troubleshoot constituent casework issues. As of September 1, TSA provided briefings and tours at 14 airports to 174 staffers from 125 congressional offices in calendar year 2016.

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	**Report Number**	**Description**	**Final Report Due**
GAO 14-37SU/14-159: TSA Should Limit Future Funding for Behavior Detection Activities	441064	GAO found that available evidence does not conclusively support that behavioral indicators can be used to identify persons who may pose a risk to aviation security. GAO provided TSA with a recommendation to limit future funding until TSA provides scientifically-validated evidence of program effectiveness. TSA non-concurred but continues to share information to GAO illustrating program enhancements. Recently, TSA successfully pilot tested revised behavioral indicators and protocols. Next, TSA expects to begin an operational test sometime in the latter half of 2016. GAO considers this to be a high priority recommendation.	Nov-2013

OIG Audits			
Title	**Report Number/Job Code**	**Description**	**Final Report Due**
OIG: Covert Testing of Passenger Security Checkpoint	16-060-AUD-TSA	OIG's objective is to covertly test passenger screening checkpoint security (both on-person and carry-on baggage).	Feb-2017
OIG: FAMS Oversight	16-019-AUD-TSA	OIG will determine the value and justification for flying Federal Air Marshals given the multiple layers of security employed by TSA.	Dec-2016

~~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.~~

OIG Audits			
Title	**Report Number/Job Code**	**Description**	**Final Report Due**
OIG: Controls Over Access Media Badges	15-099-ISP-TSA	OIG seeks to assess TSA's controls to mitigate potential risks associated with unaccounted for, lost or stolen airport issued badges.	Sept-2016
OIG: TWIC Background Checks: Not as Reliable as They Could Be	15-104-AUD-USCG, TSA	OIG evaluated the effectiveness of the TWIC applicant screening process for ensuring only eligible TWIC cardholders remain in the program. OIG found that TWIC leadership does not provide sufficient oversight and guidance to ensure effective operations. OIG made 5 recommendations. (Note: In May 2011, GAO identified TWIC internal control weaknesses and recommended an internal control assessment [GAO 11-657]. The recommendation is currently open and considered by GAO to be "high priority." TSA plans to conduct the assessment and use the results to implement effective policies and processes to meet TWIC program objectives.)	Aug-2016

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
Persistent Threats to Transportation

OVERVIEW

- The U.S. transportation sector is an enduring terrorist target based on sustained terrorist interest in the sector as demonstrated by recent international attacks on aviation and mass transit. In the first half of 2016, there were 13 attacks against civil aviation abroad, a 117 percent increase from the same time period in 2015. During this same timeframe, there were 30 attacks against mass transit assets worldwide.
- Homegrown Violent Extremists inspired by foreign terrorists pose the most likely domestic transportation threat and can use small arms and rudimentary explosive devices against airports, surface, and maritime transportation with little to no warning.
- The Department of Homeland Security (DHS) works with federal, state, local, tribal, territorial, private sector, and international partners to protect and deny terrorists access to critical transportation infrastructure. DHS continues to prioritize preventing terrorists and radicalized individuals from traveling to the United States. to launch attacks.
- There are several significant trends with respect to transportation threats:
  - Multiple terrorist groups recently conducted, planned, or attempted international aviation sector attacks and still prioritize targeting of aviation and its infrastructure.
  - Trusted transportation insiders facilitated several recent attacks on international aviation and associated infrastructure, posing an enduring concern regarding insider threats.
  - Terrorist organizations attacked public portions of the airport to cause mass casualties during recent attacks in Brussels, Belgium, and Istanbul, Turkey.
  - Terrorist networks conducted recent attacks against in-flight aviation internationally including the destruction of a Metrojet Airlines flight over Egypt's Sinai Peninsula and detonation of an explosive device aboard a Daallo Airlines flight over Somalia.
  - Terrorist groups understand the economic consequences of aviation attacks, including negative effects on tourism industries following the recent aviation-focused attacks.
  - Terrorist groups and radicalized individuals continue to engage in international attacks against surface transportation including passenger and freight rail and mass transit passengers.
- Aviation passenger and cargo operations are closed systems with interdependent security protocols, requiring each element of the security regime to perform its function to safeguard the sector. Risks to the sector include domestic or international partners failing to follow protocols and transportation insiders facilitating terrorist attacks.
- The public portions of airports and surface transportation including rail, mass transit, and highway systems do not have intensive security regimes and are optimized to facilitate the efficient flow of people and goods. These systems are more vulnerable to attack than aviation.
- DHS uses several approaches to mitigate transportation threats and applies an intelligence-driven risk-based security approach to safeguard transportation systems tailored to each specific threat. Responses may include:
  - Stakeholder information sharing initiatives.
  - Changes to security operations.

~~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.

- Enhancements to training.
- Deployment of law enforcement personnel.
- Issuing regulatory requirements for enhanced security measures.
- Foreign partner assistance.
- Providing security operations with improved technology to prevent and mitigate terrorist attacks.

DETAILED DISCUSSION

Role of DHS in Countering Transportation Threats

- DHS mission alignment for countering transportation threats:
  - DHS: Coordinates activities across the department and leads interagency efforts to mitigate threats to transportation.
  - Transportation Security Administration (TSA): Protects the nation's transportation system, regulates transportation security measures, and performs aviation passenger screening and transportation worker vetting.
  - U.S. Customs and Border Protection (CBP): Focuses on pushing the borders outward with the purpose of intercepting and addressing potential threats at the earliest possible opportunity overseas and before such threats reach the United States.
  - U.S. Immigration and Customs Enforcement (ICE): Employs immigration and customs authorities to investigate potential terrorist threats associated with criminal violations of immigration and customs regulations.
  - U.S. Coast Guard (USCG): Screens and conducts routine security compliance inspections aboard foreign flagged merchant vessels and crews entering U.S. ports.
  - National Protection and Programs Directorate (NPPD): Protects critical transportation infrastructure including cyber infrastructure and facilitates information sharing with transportation sector partners.
  - Science and Technology (S&T): Researches and develops technologies and methods that help operators detect threats.

Issue Background

- The threat to the nation's transportation systems and infrastructure from terrorism is persistent and is anticipated to remain dynamic and evolve for an extended time. Insider access to secure portions of the transportation sector poses a significant threat to comprehensive transportation security. Controlling access to the secure restricted areas of an airport, including the area beyond the TSA screening checkpoint, remains a shared responsibility among government agencies, airports, airlines, and other stakeholders. DHS employs risk-based, intelligence-driven operations in partnership with transportation stakeholders to prevent terrorist attacks and mitigate transportation risks.
- Throughout all points of the travel sequence, starting with the earliest indications of potential travel and including the inspection or arrivals process for passengers arriving from foreign points, DHS continually vets passengers and travel information, including visas and Visa Waiver Program travel authorizations. DHS matches travelers' information against government terrorist and law enforcement databases, and uses risk-based criteria developed based on actionable intelligence derived from current Intelligence Community reporting or other law enforcement information available to DHS.

~~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.~~

- The Islamic State of Iraq and the Levant (ISIL) is the preeminent terrorist threat facing transportation. ISIL attacked aviation targets claiming strikes against the Metrojet flight in Egypt, and the Brussels and Istanbul airports. ISIL also inspired radicalized individuals to conduct attacks against rail passengers in Germany and France.
- Al-Qa'ida and its affiliates continue to aspire to conduct external attacks. Al-Qa'ida in the Arabian Peninsula, in particular, has the intent and capability to attack in-flight aviation, and released issues of its *Inspire* magazine dedicated to aviation attacks.
- Maritime attacks would likely target facilities associated with government and law enforcement or high concentrations of civilians for mass casualties.
- Cyber-attacks against transportation infrastructure will most likely be limited to low level attacks against public-facing websites including web defacements and distributed denial of service attacks and are unlikely to result in destruction of critical transportation infrastructure.

Courses of Action

- During the last year, attacks against aircraft and airports in Egypt, Somalia, Belgium, and Turkey have underscored the continued threats to aviation. DHS is taking aggressive steps to enhance aviation and airport security globally. Transportation security measures include:
  - Since 2014, security at overseas last-point-of-departure (LPD) airports (generally speaking, a foreign airport from which non-stop service to the United States originates) has been strengthened, and a number of foreign governments have replicated those enhancements at non-LPD airports. Security at LPD airports remains the focus area in light of recent attacks, including those in Brussels and Istanbul.
  - In April 2015, TSA issued guidelines to domestic airports to reduce access to secure areas to address concerns about insider threats. Today, airport and airline personnel are better screened by airport operators as well as TSA, employee access points have been reduced, and random screening of personnel within secure areas has increased four-fold.
  - In 2015-2016, TSA enhanced the vetting requirements for aviation workers by requiring more frequent criminal history checks to complement the already existing recurrent terrorism vetting in place. TSA also began the implementation of the FBI's Rap Back service with two airports and one airline, which provides the capability for automatically updated criminal history checks. Full expansion of the service to additional airports and airlines is targeted to begin in late Fall 2016 as airports and airlines assess and address technical and operational requirements to support Rap Back.
  - In May 2016, TSA and airport operators completed detailed vulnerability assessments and mitigation plans for nearly 300 domestic airports.
  - DHS engages in continual information sharing to ensure all stakeholders are aware of the specific threats and recommended mitigation measures.
  - DHS Components continually assess threats and enhance visible and hidden law enforcement presence at higher threat locations, including adjustments to the deployment of TSA's Federal Air Marshal Service.
  - TSA and CBP use regulatory authorities to require threat-based security protocols for passenger and cargo flights, including TSA's issuance of Security Directives and Emergency Amendments requiring enhanced security in response to threats.

~~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 has a robust foreign training and assistance program ensuring partner preparation to counter transportation threats, including insider threats.
- USCG maintains a rigorous International Ship and Port Facility Security program that routinely assesses security standards and implementation at foreign sea ports around the world. The program allows USCG inspectors and security teams to prioritize the inspection of ships arriving to the U.S. from higher-risk ports.
- S&T is developing technologies to reduce the risk of attacks on aviation and surface transportation systems. This includes innovative approaches to find threats in cargo, in vehicles, in a person's luggage, and on someone's body.
- S&T studies threats to establish better performance requirements for current and future technologies.
- S&T provides canine training aids and testing material to better evaluate and enhance the performance of the Department's working dogs.

Key Partnerships

- DHS shares information and implements transportation threat mitigation measures in conjunction with critical partners including:
  - The transportation industry including air and maritime passenger and cargo carriers; Amtrak; and airport, rail, cruise ship, highway, and mass transit operators.
  - Federal, state, and local law enforcement partners through the DHS Fusion Centers, Joint Terrorism Task Forces, and the Intelligence Community.
  - International aviation and maritime partners including port and airport operators; the International Civil Aviation Organization; foreign transportation security organizations; and international customs and law enforcement organizations.

~~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
REAL ID

OVERVIEW

- REAL ID[1] is a coordinated effort by the states[2] and the Federal Government to improve the reliability and accuracy of state-issued driver's licenses and identification cards (ID) in order to prevent the fraudulent issuance or use of these documents and, thereby, inhibit terrorists' ability to evade detection.
  - The REAL ID Act of 2005 ("the Act") (P.L. 109-13): 1) sets minimum requirements for the secure issuance and production of state-issued driver's licenses and IDs; and 2) prohibits Federal agencies from accepting driver's licenses and IDs issued by noncompliant states for official purposes (i.e., entering nuclear power plants, accessing Federal facilities including military installations, and boarding federally-regulated commercial aircraft).
  - It does <u>not</u>: require states to participate (state participation is voluntary but there are consequences to noncompliance); create a national ID; or create a Federal database of driver information.
- DHS has expended considerable effort to advance implementation of REAL ID through coordination with Governors, and their representatives, Department of Motor Vehicle Administrators, state legislators and national state associations.
- There are some states that have taken a "wait and see" stance to see if DHS is truly serious about REAL ID implementation and as a result, DHS has established strict enforcement dates.
- In 2017, DHS will: 1) make compliance determinations for states submitting compliance certification packages; 2) grant extensions to individual noncompliant states as appropriate;[3] and 3) prepare the public for enforcement related to boarding commercial aircraft.[4]
- The statutory requirements of the Act are the main driver for DHS enforcement.[5]
  - 13 states and 1 territory are not yet committed to becoming compliant (see Table 1 and Fig. 1) and could be affected when the Transportation Security Administration (TSA) begins enforcement on January 22, 2018. At that time, TSA will no longer accept licenses issued by noncompliant states (without extensions) for boarding commercial aircraft or entering an airport's sterile area.
- Potential courses of action include: adhering to the current enforcement plan; seeking statutory and regulatory changes to reduce compliance costs identified by some of the

---

[1] Not an acronym.

[2] "State" is defined as the 50 states; the District of Columbia; and the territories of American Samoa, Commonwealth of Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands.

[3] Section 205(b) of the Act authorizes the Secretary of Homeland Security to grant states with an extension of time to meet the REAL ID requirements if the state provides adequate justification for noncompliance. Federal agencies may continue to accept driver's licenses and IDs issued by noncompliant states with an active extension.

[4] *Statement by Secretary Jeh C. Johnson on The Final Phase of REAL ID Act Implementation*. January 8, 2016. https://www.dhs.gov/news/2016/01/08/statement-secretary-jeh-c-johnson-final-phase-real-id-act-implementation#

[5] Under a 2012 interagency plan, the Federal Government has been phasing in REAL ID enforcement, an approach that has encouraged states to make progress by providing clear, realistic consequences for continued noncompliance.

~~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.~~

remaining noncompliant states; or adjusting the enforcement schedule, which may necessitate regulatory changes.

DETAILED DISCUSSION

Role of DHS

- DHS Office of Policy, on behalf of the Secretary, determines state compliance; grants extension from enforcement where justified; and provides leadership to other Federal agencies on REAL ID issues. TSA is responsible for outreach and enforcement of the Act's prohibitions related to boarding commercial aircraft. National Protection and Programs Directorate's (NPPD) Interagency Security Committee (ISC) maintains guidelines to support standardized enforcement measures across Federal agencies.

Issue Background

- The REAL ID Act was passed by Congress in response to a 9/11 Commission recommendation for the Federal Government to "set standards for the issuance of sources of identification, such as driver's licenses."[6]
- To be compliant, a state needs to: 1) require an applicant to present and for the state to verify evidence of identity, social security number, and lawful status; 2) incorporate physical security technology in the issued documents; 3) have a security plan to govern operations; and 4) meet all other requirements.
- REAL ID applies to 56 jurisdictions (see Table 1). As of September 1, 2016:
  - 24 states are compliant, and 18 noncompliant states commit to being compliant.
  - Of the 14 remaining noncompliant states: two have submitted compliance packages but have not committed to re-credentialing holders of pre-REAL ID driver's licenses and IDs; and 12 have not committed to compliance. All but four have had extensions in the cycle ending October 10, 2016.
- From 2006-2011, DHS has provided $263 million in REAL ID grants to states.[7]
- DHS is working with the remaining states to encourage compliance.
  - On average, noncompliant states[8] meet 84% of the REAL ID requirements.
  - Barriers to compliance in some states include the cost to re-credential pre-REAL ID driver's license holders and the need to enact state legislation to enable compliance.
  - For states that continue to make progress, DHS grants up to 1-year extensions (renewable). By policy, the progress needed for a state to receive an extension increases each year so that it is not a long-term alternative to compliance.
- Enforcement for boarding commercial aircraft will occur in two phases (see Fig.2):
  - Starting January 22, 2018, TSA will not accept licenses or ID cards from *noncompliant states that do not have an extension*.[9] Passengers with such licenses will need to present alternative documents (e.g., Passport, military ID).

[6] The Commission found that the 19 hijackers had been issued 16 state driver's licenses and 14 state IDs. Two hijackers were unlawfully present in the United States when they obtained driver's licenses and/or IDs.
[7] After 2011, the Driver's License Security Grant Program was subsumed by a block grant.
[8] Excluding American Samoa, which has not submitted data.

~~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.~~

- By regulation, starting October 1, 2020, TSA will not accept *noncompliant* licenses or ID cards from *any* state. Passengers will need a REAL ID-compliant license or ID card, or other acceptable identification, to board aircraft.[10]

- REAL ID enforcement may have a significant impact on the commercial aviation sector, as TSA screens over 2 million passengers daily. If even one noncompliant state does not have an extension on January 22, 2018, a significant number of U.S. citizens may have difficulty presenting an appropriate identification document at TSA security checkpoints, which could impact their ability to fly domestically.[11]

Courses of Action

1. **Adhere to current enforcement plan** – The phased enforcement plan has led to many states making progress toward achieving full compliance. The current strategy is to continue working with states to become compliant using the upcoming TSA enforcement as a major driver to encourage compliance.[12]
2. **Reduce compliance costs for states** Some noncompliant states' concerns over the costs for implementing REAL ID could be addressed by seeking: 1) Congressional authorization to limit the scope of the population to be re-credentialed on a risk basis;[13] and/or 2) appropriations to award new REAL ID grants. DHS also could amend the regulations to potentially reduce costs under existing law. However, previous attempts to request Congressional modifications to the Act were not successful, sent mixed messages about DHS' interest in enforcement and actually served to discourage state progress towards full compliance. The consequences of seeking legislative or regulatory changes would likely remain and even heighten given progress on enforcement as well as state efforts towards achieving full compliance.
3. **Adjust the enforcement schedule** – The phased enforcement schedule was established as a way to progressively roll out REAL ID enforcement with the consequences of noncompliance becoming more pronounced with each enforcement phase. The schedule culminates with TSA enforcement beginning in January 2018 and the full regulatory enforcement date of October 2020. Adjusting the phased enforcement schedule or amending the October 2020 regulatory full compliance date would provide some relief to the remaining noncompliant states; however, it would increase the risk of states inferring that TSA enforcement will never begin, impacting their progress in becoming compliant. It also risks DHS' credibility in REAL ID enforcement as we are close to a decade out from the statutory enforcement date.

---

[9] Passengers with driver's licenses issued by a state that is compliant with REAL ID (or a state that has been issued an extension) will still be able to use their state-issued identification.

[10] See 6 C.F.R. § 37.5 (2014) (extending aged-based enforcement deadline to October 1, 2020).

[11] TSA does not anticipate that all passengers will acquire and carry alternative identification for domestic travel when REAL ID enforcement begins at airport security checkpoints.

[12] The Act called for enforcement to begin in 2008. Through amendments to the regulations and phased enforcement, TSA enforcement will begin in January 2018. These extensions give states a reasonable amount of time to become compliant, which in some cases involves changes in state statutory and regulatory authorities, as well as investments in staff training and information technology.

[13] Such as excluding persons who have held licenses and IDs with the state for ten or more consecutive years.

~~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

- All Federal agencies.
- The House and Senate Appropriations Committees; the House and Senate Homeland Security Committees; and State Congressional delegations.
- State governors, legislatures, homeland security advisors, and driver's licenses issuing agencies – along with their respective associations.
- Travel, tourism, and hospitality industry; airports; air carriers; and individuals who use their driver's licenses and IDs for official purposes.

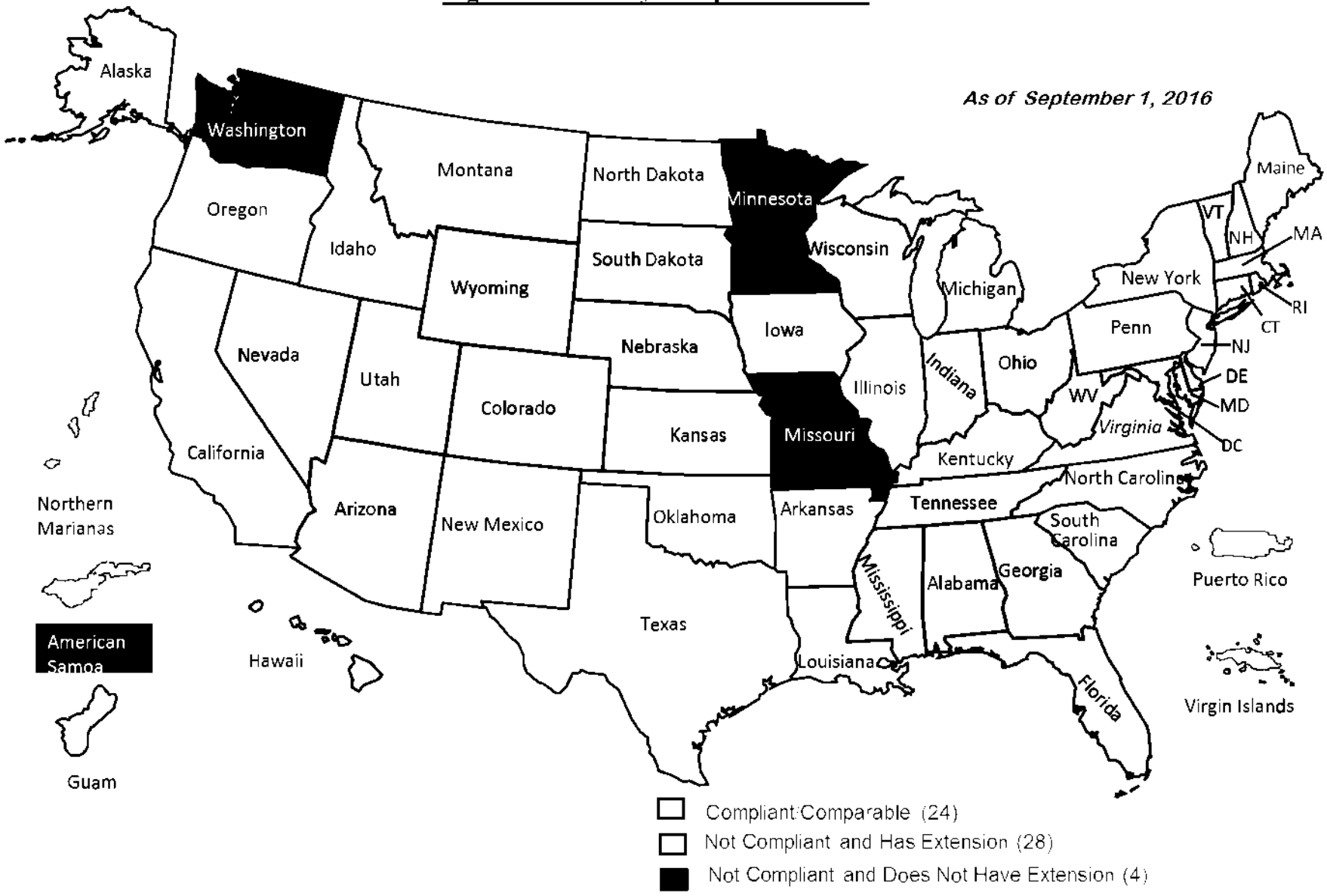
Table 1: Status of States (September 1, 2016)

COMPLIANT (24)		**NONCOMPLIANT (32)**			
		Extension (28)			**No Extension (4)**
		Plans to Meet All Standards (18)	*Has Not Committed to Meeting All Standards (14)*		
Alabama	Maryland	Arkansas	California*	Alaska	Minnesota
Arizona	Mississippi	Idaho	Virginia *	Kentucky	Missouri
Colorado	Nebraska	Illinois		Maine	Washington
Connecticut	Nevada	Louisiana		Montana	*American Samoa*
Delaware	Ohio	Massachusetts		Oklahoma	
District of Columbia	South Dakota	Michigan		Oregon	
Florida	Tennessee	New Hampshire		Pennsylvania	
Georgia	Utah	New Jersey		South Carolina	
Hawaii	Vermont	New Mexico			
Indiana	West Virginia	New York			
Iowa	Wisconsin	North Carolina			
Kansas	Wyoming	North Dakota			
		Rhode Island			
		Texas			
		Guam			
		Northern Marianas			
		Puerta Rica			
		Virgin Islands			
34%		*35%*	*16%*	*9%*	*6%*
Percent of U.S. Population					

* Submitted compliance package but has not committed to meeting all standards for re-credentialing.

~~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.~~

Figure 1: States by Compliance Status



~~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.~~

Figure 2: Comparison of Acceptable State-issued ID in Initial v. Final Phases of Aviation Enforcement

	Compliant license from a compliant state	Noncompliant license from a compliant state	License from a noncompliant state with an extension	License from a noncompliant state without an extension
(b)(6)				
Initial Phase 01/22/2018	Accepted	Accepted	Accepted	Not Accepted
Final Phase 10/01/2020	Accepted	Not Accepted	N/A	Not Accepted

~~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.~~

RFI 090 TSA Attrition Rates Summary

TSA Attrition Rates by Year

FY	FY	FY	FY
2013	2014	2015	2016
11.74%	12.89%	13.39%	14.08%

Full Time and Part Time TSO Attrition Rates by Year

FY2013 FT Attrition Rate	FY2013 PT Attrition Rate	FY2013 TOTAL Attrition Rate	FY2014 FT Attrition Rate	FY2014 PT Attrition Rate	FY2014 TOTAL Attrition Rate	FY2015 FT Attrition Rate	FY2015 PT Attrition Rate	FY2015 TOTAL Attrition Rate	FY2016 FT Attrition Rate	FY2016 PT Attrition Rate	FY2016 TOTAL Attrition Rate	FY2017 FT Attrition Rate	FY2017 PT Attrition Rate	FY2017 TOTAL Attrition Rate
8.8%	25.5%	13.3%	10.2%	28.7%	14.6%	10.6%	26.9%	14.2%	11.7%	30.6%	15.7%	10.8%	29.4%	14.7%

Notes:

~~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 unauthrized members of the elect President - 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.~~

Fiscal Year	Headcount at End of Fiscal Year	Total Separations for FY	Attrition Rate
2013	64,152	7,530	11.74%
2014	61,140	7,884	12.89%
2015	58,827	7,877	13.39%
2016	61355	8,641	14.08%

5. What IT equipment has been purchased but is not in use.

High Volume Assets Located at Springfield, VA Warehouse as of December 9, 2016			
Type	**Quantity**	**Responsible Organization**	**Explanation of Volume on Hand**
Switches	759	OED	All purchased IT infrastructure equipment not currently in use are to be used for in-flight infrastructure projects such as the FLETC buildout, EDS inline infrastructure upgrades, and Mission Net support projects, in addition to replacement components for break/fix O&M activities.
Servers	47	OED	All purchased IT infrastructure equipment not currently in use are to be used for in-flight infrastructure projects such as the FLETC buildout, EDS inline infrastructure upgrades, and Mission Net support projects, in addition to replacement components for break/fix O&M activities.
Laptops	508	EUSD	Inventory to be leveraged for the ongoing Enterprise Computer Refresh Deployment to be completed by June 17.

~~**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 elect President- 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.**~~

Desktops	90	EUSD	Inventory to be leveraged for the ongoing Enterprise Computer Refresh Deployment to be completed by June 17.
Land Mobile Radios	606	EUSD	Legacy radios returned as part of the LMR Refresh Project; Spare equipment to be transferred to other Agencies at end of project.
Printers	828	EUSD	Inventory to be leveraged for the ongoing Enterprise Printer Refresh Deployment to be completed by June 17.
Fax Machines	195	EUSD	Inventory to be leveraged for the ongoing Enterprise Fax Refresh Deployment to be completed by June 17.
Plotters	61	EUSD	Inventory to be leveraged for the ongoing Enterprise Plotters Refresh Deployment to be completed by June 17.
Scanners	149	EUSD	Inventory to be leveraged for the ongoing Enterprise Scanners Refresh Deployment to be completed by June 17.

~~**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 elect President- 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.**~~

High Volume Assets Located at Coppell, TX Warehouse as of December 9, 2016			
Type	**Quantity**	**Responsible Organization**	**Explanation of Volume on Hand**
Laptops	11900	EUSD	Inventory to be leveraged for the ongoing Enterprise Computer Refresh Deployment to be completed by June 17.
Desktops	200	EUSD	Inventory to be leveraged for the ongoing Enterprise Computer Refresh Deployment to be completed by June 17.

~~**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 elect President- 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.**~~

TSO Basic Training Overview

TSA Academy Delivery	
Total Curriculum Training Hours	80
Training Environment	The FLETC Glynco facility is an accredited training center, and establishes a formal/structured learning environment. As FLETC is a training facility for DHS components focused on law enforcement, counter-terrorism and security, new hire TSOs are able to establish a connection to the DHS mission through networking and interaction with other agencies. This brands TSOs as national transportation security professionals. New hire TSOs establish a connection to TSA from locations throughout the nation. This builds an esprit de corps and provides them with a TSA institutional identify rather than an airport identify. The TSA Academy simulates a fully operational checkpoint environment and provides scenario-based, hands-on training.
TSA Indoctrination Process	**Instructor-Led Training:** – TSA Overview – Aviation Security – Terrorist Threat – Professional TSO – Airport Overview – Effective Communication – Passenger Engagement – Social Engineering
Equipment: Hands-on Training	**Hands-On Training:** – Introduction to the screening equipment TSOs will operate specifically at their local airport: Advanced Imaging Technology (AIT), Walkthrough Metal Detector, x-ray, and Explosives Trace Detection (ETD) equipment introduction. – Scenario-based learning operating equipment and practicing procedures in a fully-equipped checkpoint.
X-ray Image Interpretation Training	**Interpretation Training:** Progressive instruction that starts with common items, builds to focus on prohibited items, then culminates in targeted IED recognition training.

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized TSA official. No portion of this report should be furnished to the media, either in written or verbal form.

TSA Academy Delivery	
Procedural/SOP Focused Curriculum	Scenario-based learning with structured content targeted at skill-building and practical application for each screening process. – Lessons for screening persons begin with clarity on the processes associated with Standard Screening, then builds to those persons requiring additional screening, then builds to screening of individuals with disabilities, and then introduces changes that support risk-based screening procedures and the why behind each of these different categories of screening persons.
Demonstration of Effects of Improvised Explosive Device (IED) Detonation	Academy delivery permits access to the FLETC demolition range, where Transportation Security Specialists –Explosives (TSS-Es) detonate IEDs built to replicate actual threats that have been encountered.
Intelligence Briefing	All new hire TSOs will receive an unclassified intelligence briefing from a Field Intelligence Officer about the current threat to aviation security.
Active Shooter Drill	All new hire TSOs will experience a simulated active shooter scenario within the checkpoint setting.

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized TSA official. No portion of this report should be furnished to the media, either in written or verbal form.

Summary of Changes

Date	Line #	Update that occurred
7-Sep-16	10300	Per OSO, the item (DO tng) has been changed to a one-time requirement (that is only applicable to newly certified officers)
15-Sep-16	ALL	OLC Item codes were added
15-Sep-16	11000	Mission Essentials: Alarm Resolution was moved to a QTR1 release
15-Sep-16	10900	Mission Essentials: Terrorist Planning Cycle was moved to a QTR 2 release
15-Sep-16	10800	Reflects updates due to TCU 20160909-0048
15-Sep-16	10801	Reflects updates due to TCU 20160909-0048
15-Sep-16	10802	Reflects updates due to TCU 20160909-0048
23-Sep-16	21400	Item removed due to a duplicate item in item line 21000
28-Sep-16	10100-10115	Updated OLC course codes
28-Sep-16	10700	Removal of assignment from bag officers
4-Oct-16	20500	Course Item/removed per the BDO program office
20-Oct-16	21205	OLC Item code was updated
10-Nov-16	18	Course content was not updated thus it has been removed from the FY17 NTP (the training is still required as a one-time occurrence for all officers and is not a recurrent training item)
15-Nov-16	20300	~~Course Item/removed per the BDO program office~~
15-Nov-16	20900	Course Item/removed per the BDO program office
16-Nov-16	12	OLC Item code was updated
18-Nov-16	20100-10103	Completion Oate Changed to January 31, 2017 (TM/TS message 20161117-0201)
28-Nov-16	20300	Course Item was restored to the NTP per the BDO program office

~~(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized TSA official. No portion of this report should be furnished to the media, either in written or verbal form.~~

DHS Presidential Transition Landing Team Questions for TSA #096

096. Please provide all training information including consequences for failing training.

TSA's Office of Training and Development (OTD) is responsible for providing the full range of training and development functions to TSA employees to ensure successful execution of the Agency's mission and professional development of its employees.

I. New Hire and Recurrent Training:

The workforce has been categorized into three distinct populations for New Hire and Recurrent Training: (1) Security Operations Personnel, (2) Law Enforcement Personnel, and (3) Management and Administrative Professional (MAP) Personnel. Training specific to each group is designed to refine the requisite technical skills and strengthen subject-matter expertise for enhanced performance

A. Security Operations Population

Transportation Security Officer (TSO) Training:

Pursuant to the Aviation and Transportation Security Act (ATSA), all Transportation Security Officers (TSO) are required to attend and pass the Transportation Security Officer Basic Training Program (TSO-BTP) and On-The-Job Training to be certified to screen passengers and checked baggage. (See Attachment 1 for key elements of the TSO-BTP curriculum.) Attendance is required within four weeks of onboarding. TSO-BTP is 80 hours. TSO-BTP is delivered at the TSA Academy on the Glynco, Georgia, campus of the Federal Law Enforcement Training Center (FLETC). New hires who fail to successfully complete the testing associated with TSO-BT, are provided remediation focused on the area(s) where they failed. If the new hire fails the retest after remediation, he or she is returned to their home airport where they receive their termination notice.

TSOs will average approximately 45-60 hours of required annual training, typically at their home airports, to ensure they maintain proficiency in the skills learned during TSO-BTP. TSA established an annual National Training Plan (NTP) to meet this objective. (See Attachment 2 for the FY17 NTP.) It includes hands-on instructor-led training courses in support of technical training, and relies on computer-based online training to meet administrative and general training requirements. Training that is developed to support Standard Operating Procedure changes, deployment of new technologies, and/or operational changes to currently deployed technologies, is issued throughout the year as needed. Each year there is a block of training time that is identified within the NTP as a place holder for those training events that are not yet known when the NTP is published at the beginning of each FY.

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 elect President- 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.

All TSOs must also successfully complete a required Annual Proficiency Review (APR), to include assessments such as a Practical Skills Evaluation and Image Mastery Assessment. This is a condition of their employment per ATSA. TSA offers remediation and re-assessment opportunities for all TSOs who fail an assessment on the first and/or second attempt. TSOs who do not successfully complete their APR are subject to removal from TSA. It is TSA's policy to make every attempt to re-train, mentor and assist TSOs who fail an assessment in order to return them to active status as soon as possible.

Newly appointed Lead TSOs, Supervisory TSOs, and Transportation Security Managers (TSMs) are required to attend training within six months of promotion. This training is accomplished presently through the Essentials of Leading/Supervising/Managing Screening Operations series of courses. Additionally, Assistant Federal Security Directors (AFSDs) are required to attend training within six months of appointment.

Canine Training:

The Canine Training Center (CTC), located on Lackland Air Force Base in San Antonio, TX, conducts initial, annual recurrent and remedial canine evaluations. It provides extensive instructor-led training consisting of 21 combined weeks of canine and canine handler training for Explosive Detection Canines (EDCs) and 32 combined weeks for Passenger Screening Canines (PSCs). In FY16, approximately 230 new canine teams were trained and an additional 833 existing canine teams underwent evaluation. If a student does not satisfactorily meet the training standards, he or she is removed from the course and returned to their assigned duty station where a final status determination is made. The TSA anticipates that close to 300 new canine teams will be trained in FY17.

B. Law Enforcement Personnel

Federal Air Marshals (FAMs) are required to complete FAM basic training. The training totals approximately 16½ weeks of instruction through the FAM Training Program (FAMTP), which is comprised of two components. FAMTP-I is delivered by FLETC staff at its Artesia, New Mexico, campus, while FAMTP-II is conducted at the TSA Training Center in Atlantic City, New Jersey (TSATC). FAMs who do not successfully complete their basic training are subject to removal from TSA.

FAMs also have a robust and dynamic annual recurrent training requirement of 160 hours at the FAMS Field Offices. TSA policy sets quarterly, bi-annual, and annual recurrent training requirements for all FAMs, and failure to achieve the standards established for this training will result in a FAM being removed from active mission status until he or she achieves a passing status.

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 elect President- 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.

C. Management and Administrative Professional (MAP) Population

The MAP Basic Training Program is mandatory for all newly hired MAP employees, effective January 2017. Its requirements were developed jointly by contributors from OTD, the Office of Security Operations (OSO), the Office of Human Capital (OHC), and other key stakeholders. This in-residence training at TSATC builds a foundational common culture and improves performance by standardizing training for new MAP employees. Moreover, the training instills in attendees a true sense of how MAP employees support the frontline Officers and why their contribution to the mission is so critical. To reinforce that point, a visit to nearby Philadelphia International Airport (PHL) is included in the MAP Basic Training Program. MAP personnel also must satisfy initial and annual recurrent training requirements through job-specific instruction (e.g., acquisitions, information technology, and intelligence). The MAP course is not designed to be a pass or fail course.

II. Mission-Focused Leadership Training:

Starting in January 2017, as employees are promoted to J-Band positions and above, TSA leverages partnerships with Institutions of Higher Education (IHEs) to provide mandatory leadership training. The intent is to enhance leadership skills that align with the Office of Personnel Management's (OPM) Executive Core Qualifications (ECQs), and to promote continuity of themes, expectations and language along the entire leadership training progression.

A. Mandatory Training Upon Promotion to J-Band and K-Band

TSA partnered with accredited IHEs to develop and deliver a mandatory program for J-Band and K-Band employees within six months of promotion to provide a multi-disciplinary approach that emphasizes leadership in a risk-based security environment and cultivates their OPM ECQs.

B. Mandatory Training Upon Promotion to L-Band

Within six months of promotion, all L-Band employees are required to attend the Federal Executive Institute's (FEI) Leadership for a Democratic Society course in partnership with OPM.

C. Mandatory Training for Newly Promoted TSES Employees

All Transportation Security Executive Service (TSES) employees are required to attend training within six months of promotion. TSA will collaborate with an IHE partner to develop and deploy an executive leadership program that includes development of a leadership development plan and executive coaching for assessment, feedback, and support.

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 elect President- 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.

D. Mandatory Recurrent Training for Current TSES Employees

Incumbent TSES employees are required to complete specified mission-focused professional development training every three to five years to reinforce and maintain leadership competencies. The recurrent training consists of a one-week in-residence session and executive coaching for TSES leaders.

E. Mandatory Training for Newly Promoted and Current FSDs

All Federal Security Directors (FSDs) and Deputy FSDs (DFSDs) are required to attend the FSD Training Course (formerly known as the "FSD Academy") within six months of appointment, as well as recurrent training annually thereafter. This phased curriculum incorporates leadership principles, incident and risk management, operational and performance management, and stakeholder engagement and planning. The courses are expected to be delivered at TSA Headquarters as many of the modules require sustained personal engagement with the Administrator and Senior Leadership Team.

~~**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 elect President- 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 Presidential Transition Landing Team Questions for TSA #097

097. Do all passengers entering a pre-check lane have their identity verified? Please explain.

All passengers who appear to be 18 years old or older entering a TSA Pre✓® lane must have their identification, along with their travel boarding pass, verified before they are allowed entrance into the screening checkpoint or sterile area.

To verify identification, the individual must present an acceptable form of ID with a photo that is a true representation of the individual. The ID is also checked for an expiration date that is in accordance with Acceptable Forms of ID Policies. In addition, the ID is also checked for security features to verify the ID is not fraudulent.

If a person does not have an acceptable form of ID, the identification of the individual can be verified via other processes, such as the TSA Identity Verification Call Center (IVCC) process, which utilizes commercial databases to confirm identity. In these instances, the passenger is redirected to a standard screening lane and receives additional screening.

If further clarification is needed or we did not answer the intent of the question please notify us.

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 elect President- 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 Presidential Transition Landing Team Questions for TSA #098

098. Please provide a copy of the tiger team final report, resulting from the 2015 DHS OIG covert testing, along with the current status on all actions and recommendations?

The tiger team final report is a classified document. TSA can provide a briefing on the report in a closed session. Attached is the status as of September 2016 on all tiger team actions and recommendations. All actions and recommendations from the Tiger Team report are either closed out or been transitioned to projects. Each project is assigned to an Assistant Administrator as the Theme Lead. The Deputy Chief of Staff and Administrator's Action Group meets with each Theme Lead on a quarterly basis to assess and update the status of all projects. The next Tiger Team update will be available in mid-January.

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 elect President- 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 Presidential Transition Landing Team Questions for TSA

RFI099: Please provide any existing studies, reports, or analyses conducted within the last four years related to moving TSA employees to the GS schedule including title 5 applicability.

Answer: No studies exist at this time

~~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 elect President- 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.~~

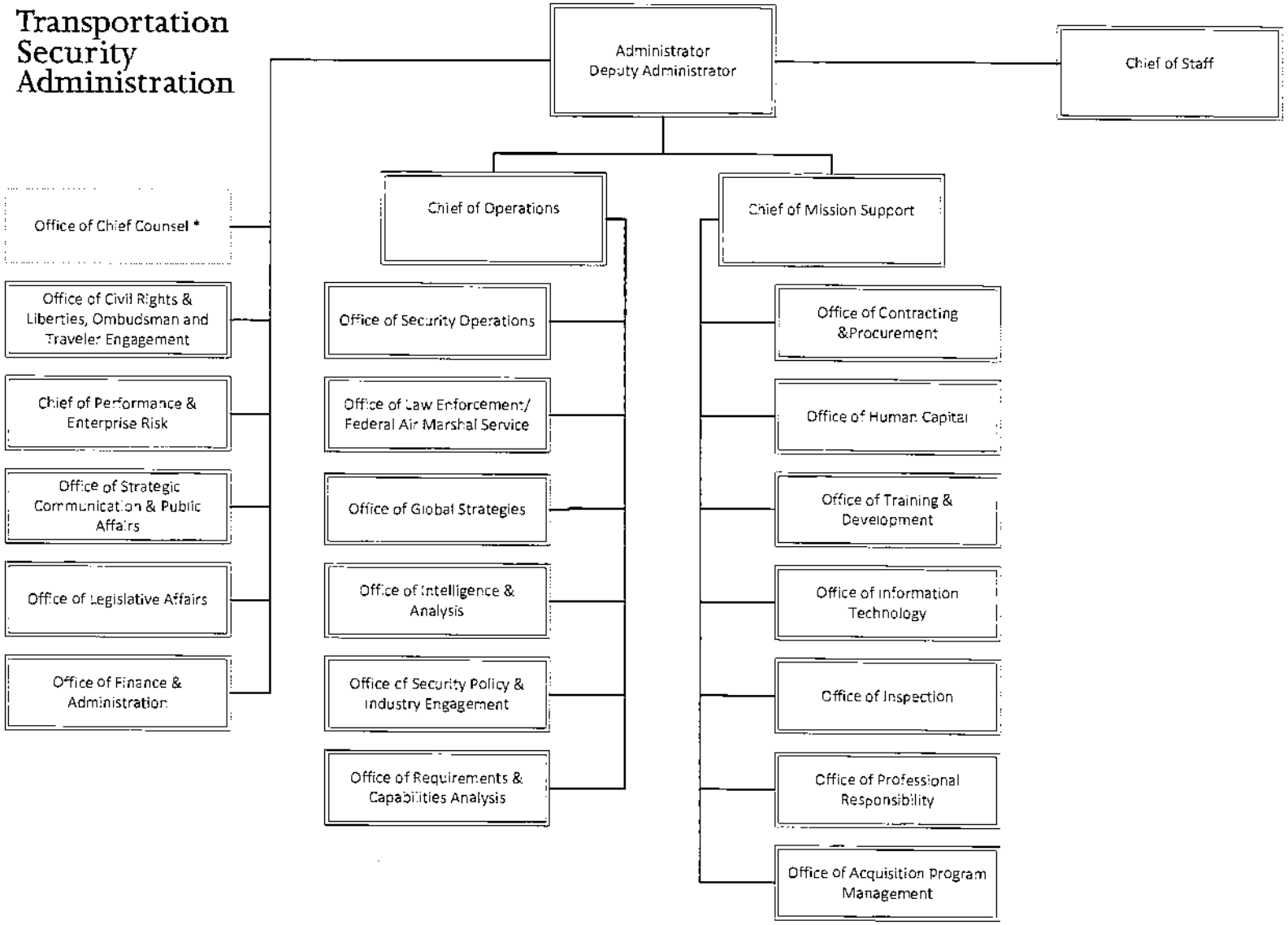
DHS Presidential Transition Landing Team Questions for TSA #103

103. Please provide any pending and/or planned organizational changes including rationale and associated funding.

Response: On October 17, 2016, TSA enacted the attached organizational structure. No future organizational changes are pending or planned at this time.

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 elect President- 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.

Transportation Security Administration



*The Office of the Chief Counsel reports to the Department of Homeland Security, Office of the General Counsel

Approved by: Huban A. Gowadia
Deputy Administrator

Signature:

Date: 17 Oct 16

DHS Presidential Transition Landing Team Questions for TSA

104. Please provide the final 2016 measures of effectiveness used by TSA's senior leadership team along with any weekly, monthly, and quarterly updates during the year.

Response: The measures of effectiveness for the past fiscal year are presented in the attached Adobe .pdf document. Each update is shared with all FSDs and senior leadership, via a conference call with TSA field personnel to review the previous month's report, share best practices, provide support, and solicit improvements. OSO Senior Leadership also schedules a detailed review of the monthly data with Regional Directors. This review includes sharing improvement efforts and corrective actions at an airport level with senior leadership and a validation of efforts with HQ Directors.

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 elect President- 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.

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation Security Administration

NOV 2 9 2016

ACTION

MEMORANDUM FOR: Huban A. Gowadia, Ph.D.
Deputy Administrator

FROM: Latetia Henderson /s/
Assistant Administrator
Office of Acquisition

SUBJECT: Acquisition Reform Task Force Charter

Purpose

To request your signature on the enclosed Transportation Security Administration (TSA) Acquisition Reform Task Force (ARTF) Charter, which identifies the mission, scope, and responsibilities of the ARTF to recommend an Agency path forward for acquisition program management. This document has been coordinated with the Core executives.

Background

Over the last 18 months, TSA embarked on an effort to assess and recommend improvements of the current requirements and acquisition management organizations, processes, and personnel. Three primary assessment efforts were undertaken: two conducted internally and one by the Defense Acquisition University (DAU). All three assessments yielded the key finding that the current acquisition program structure/organization does not support effective and efficient acquisition processes.

As a result of these assessment efforts, the ARTF was established to recommend/implement changes to TSA's acquisition program management organizations and processes. The ARTF will serve as the executive agent to transform and restructure the current acquisition management processes, organizations, and respective personnel to improve efficiency and effectiveness. The ARTF will recommend changes to the current acquisition program management organization and implement those items approved by the TSA Senior Leadership.

Recommendation

That you approve and sign the attached ARTF Charter.

Approve _____ \ 28 NOV 16 Disapprove _____ \ _____
Date Date

Modify _____ \ _____ Need more discussion _____ \ _____
Date Date

Attachment:
Acquisition Reform Task Force Charter

CHARTER FOR TSA
ACQUISITION REFORM TASK FORCE

October 2016

I. PURPOSE

Through this charter, the Transportation Security Administration (TSA) establishes the Acquisition Reform Task Force (ARTF) and describes the mission, roles, and responsibilities of membership therein.

II. MISSION STATEMENT

The TSA Administrator and Deputy Administrator (DA) established the ARTF to serve as the Executive Agent to institute a comprehensive restructuring of the Agency's Acquisition Management processes, structure, and personnel to effectively and efficiently support TSA's mission.

III. SCOPE

The ARTF will conduct analyses of TSA's overall Acquisition Management processes and structure in order to identify and recommend process improvements, and organizational structure to improve TSA's Acquisition Management. The ARTF will also prepare all necessary documentation to support implementation of organizational changes. The ARTF will leverage the related Enterprise Risk Steering Committee (ERSC) and Defense Acquisition University's (DAU's) study recommendations as a starting point to review and make recommendations on process improvements and supporting organizational structure to transition to a new acquisition organization structure. Transition elements include existing and emerging acquisition programs, personnel, and funding.

The ARTF will seek to complete work within a period of one calendar year, but will continue until Major Objectives are met.

IV. MAJOR OBJECTIVES

The DA charged the ARTF with four major objectives:

CHARTER FOR TSA
ACQUISITION REFORM TASK FORCE

1) Stand up Program Executive Offices (PEO) supported by related Program Management Offices (PMO)
   The ARTF shall leverage the ERSC/DAU recommendations to identify, recommend, and implement an approach to logically establish PEO organization(s), including subordinate PMOs, within a single office. The final definition of the identified organizational structure shall consider the required staffing for each PEO, PMO, and the leadership required to support the structure. The ARTF will develop or revise acquisition business processes across TSA to support the establishment of the PEO organization(s), and will develop or revise Management Directives (MD) and Delegations of Authority.

2) TSA Testing Office
   The ARTF shall identify, recommend, and implement an approach to logically define the location and composition of the Agency-wide Operational Test Authority (OTA) within TSA's organizational structure. This analysis will consider the tradeoffs associated with Developmental and Operational Testing and how to best address concerns associated with Test & Evaluation (T&E) independence, the necessity of test and evaluation responsibility and expertise to be present within program offices, and continuously improving TSA's department-leading T&E capability. As necessary, the ARTF will develop or revise T&E business processes and any applicable MDs and Delegations of Authority.

3) Chief Technology Officer (CTO)
   The ARTF will identify, recommend, and implement an approach to logically update the CTO primary roles, responsibilities, composition, and organizational location within the future TSA acquisition management structure. As necessary, the ARTF will develop or revise CTO business processes and any applicable MDs and Delegations of Authority.

4) Deployment and Logistics Operations
   The ARTF will identify, recommend, and implement an approach to update the organizational location for acquisition program and possible Agency-wide deployment and logistics operations. The ARTF will consider both centralized and de-centralized models for acquisition program Integrated Logistics Support. As necessary, the ARTF will develop or revise Deployment and Logistics business processes and any applicable MDs and Delegations of Authority.

For each of these objectives, the ARTF will develop recommendations and, where appropriate, implement plans to achieve each of the major outcomes. The ARTF will define metrics for reaching Initial, Transitional, and Full Operating Capability (FOC) under the new structure. The ARTF will meet FOC when the above objectives have been completed and approved by the Core Member Assistant Administrators (AA) and the DA.

V. RESPONSIBILITIES

The ARTF shall identify recommendations and implement the Acquisition Management system best suited to accomplish TSA mission requirements. As such, the ARTF membership is responsible for the following:

- Representing the interests of TSA in defining the future Acquisition Management organizational structure
- Providing insight and information to all stakeholders regarding the distinction between Acquisition and Operational Programs; using information from all stakeholders to differentiate between Acquisition and Operational Programs
- Designing and implementing acquisition organizational structures and business processes that accomplish the following activities:
    - Program Management
    - Systems Engineering
    - Integrated Deployment and Logistics
    - Emerging Technology
    - Program Test and Evaluation
- Identifying future state position qualifications and staffing requirements for Acquisition Management within the appropriate TSA Office
    - Location / Movement of Acquisition Management Staff
    - Staff Band / Skills for new organization (including required acquisition workforce certifications)
    - Oversight and Management resources required for the new Office
- Coordinating with TSA Head of Contracting Activity (HCA) to determine effective COR management in conjunction with new acquisition management organization(s)
- Designing acquisition business processes to integrate with TSA Chief Financial Officer (CFO) and Chief Information Officer (CIO) planning, programming, budgeting, and execution processes

- Coordinating with the CFO to re-align current-year and future-year budgets to the new organizational structure
- Establishing plans, procedures, and processes to establish the organization identified by the ARTF

The ARTF membership shall ensure transparency of all plans to the Core Member AAs. This will ensure that all TSA Offices are informed in the process of enhancing the Agency's Acquisition Management.

The ARTF shall coordinate with the TSA Chief Operating Officer (COO) or COO designee(s) to ensure synchronization with efforts to establish an Office of Requirements and Capabilities Analysis (ORCA) or similar TSA organization.

VI. MEMBERSHIP

As outlined in the DA's request for ARTF participation, membership is directed to be J/K-band representatives from all TSA Offices. ARTF members are nominated by their AA/Deputy AA (DAA). Each TSA Office has the opportunity to designate members to the ARTF. AA/DAAs may name members from their offices who best represent the interest of each office, regardless of pay band.

The ARTF seeks a broad range of input to enhance the implementation of a new Acquisition Management organization.

TSA Offices may update their ARTF representation. Any proposed change shall be submitted to the ARTF Chair by the appropriate AA/DAA (or their delegate). The Chair will review the proposed change and rationale to ensure the best fit for the ARTF. The Chair will discuss any concerns with the respective AA/DAA or Core Member AAs as necessary.

Each TSA Office may designate up to two official ARTF members. Members are responsible for any additional coordination required by their respective office.

The ARTF Chair is named by the DA/Component Acquisition Executive (CAE). The Chair will direct all ARTF activities and have oversight of any and all ARTF support functions. The Chair will consider input from all

membership and have final decision authority regarding recommendations/decisions (in the cases of disagreement within the membership) presented to the Core Member AAs.

ARTF Core Members are required to commit to full-time support of the effort for up to one year (or until Major Objectives are met). Core Members represent the Office of Acquisition (OA), the Office of Human Capital (OHC), the Office of Intelligence and Analysis (OIA), the Office of Information Technology (OIT), the Office of Requirements and Capability Analysis (OCRA), and the Office of Security Operations (OSO).

Additional ARTF members may come from all other TSA Offices. Each Office may name member(s) to the ARTF to provide different points of view and keep the other office appraised of the team's effort. Additional members are not required to serve full-time on the ARTF. Additional members should advise the ARTF Chair of the level of their time commitment upon joining the ARTF.

VII. GOVERNANCE AND PROCEDURES

a. Governance:
- The Core Member AAs shall provide governance and oversight to the ARTF. All outcomes and decisions of the ARTF are subject to Core Member AA review.

b. Procedures:

Meetings and Attendance
- The ARTF shall convene twice weekly, or as determined by the ARTF Chair. Meeting invites will be sent with as much notice as possible. Meetings may be called with short notice to address rapidly arising issues.
- Attendance at meetings shall be in-person. If a member cannot attend a meeting, he or she should review the notes of the meeting and bring any questions or concerns to the ARTF Chair.
- Members are expected to have reviewed all pre-meeting materials prior to the appointed meeting times.
- ARTF meetings should be attended by designated members only. Meeting invitations and notices shall not be forwarded to other TSA staff.

Task Force (TF) members are the conduit of TF information to their respective offices.

Decision-making Process

- Members shall provide the perspective and detail of their respective Office to the ARTF. All points of view shall be considered by the full body in an effort to achieve the best result for the Agency.
- The ARTF shall function as a collaborative organization and will work to achieve consensus prior to making decisions and/or recommendations. In the event that the TF is unable to reach a consensus, the ARTF Chair will raise the issue and/or recommendations as appropriate through the Core Member AAs for resolution.

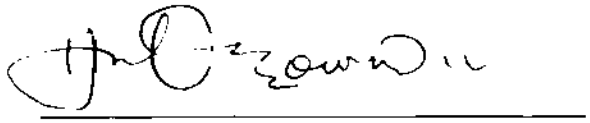
ARTF Reports and Briefings

- Reports and Briefings will be developed by assigned members and reviewed by the complete ARTF.
- Chair (with assistance from TF members) shall present all findings and recommendations to the Core Member AAs.
- All documentation shall be archived on the designated TSA iShare page, with pre-decisional and draft material restricted to the ARTF membership.

VIII. EFFECTIVE DATE

This charter is effective upon signature by the Sponsor.

IX. SPONSOR SIGNATURE



28 NOV 2016

Huban A. Gowadia, Ph.D.
Deputy Administrator
Transportation Security Administration

Date

DHS Presidential Transition Landing Team Questions for TSA

201. Provide the Acquisition Reform Implementation Plan.

Core components of an implementation plan are captured in the charter for the Acquisition Reform Taskforce, attached.

~~**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 elect President- 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.**~~

Surface Transportation Vulnerability Assessments and Security Plans
Advance Notice of Proposed Rulemaking (ANPRM)

WHITE PAPER
December 22, 2016

Proposed Rule Requirements

This rulemaking will implement the 9/11 Act requirement that higher-risk public transportation agencies, railroads (freight and passenger), and over-the-road bus (OTRB) companies conduct vulnerability assessments and security planning.

Through this rulemaking, TSA intends to solidify the enhanced baseline of surface transportation security by improving and sustaining comprehensive security programs by higher-risk public transportation systems, railroad carriers (passenger and freight), and OTRB owner/operators that include assessment of vulnerabilities for operations and nationally critical assets and infrastructure and security planning.

TSA is issuing an ANPRM to solicit sufficient data regarding the security measures industry currently employs to ensure that future proposed rules reflect the current baseline and operational environment as well as the potential impact of regulations on operations. Requesting this data is necessary to comply with minimum standards established by the Office of Management and Budget (OMB) under Executive Order 12866, and related OMB guidance, which include conducting a robust analysis of the existing baseline of persons potentially affected by a proposed rule.

Summary of Information Requested

In the ANPRM, TSA is seeking information on:

- Existing practices, standards, tools or other resources used or available for conducting vulnerability assessments and developing security plans;
- Existing security measures, including measures implemented voluntarily or in response to other regulatory requirements; and
- The scope and cost of current security systems and other measures used to provide security and mitigate vulnerabilities.

TSA is particularly interested in data from surface transportation owner/operators who currently have security plans specifically based on a vulnerability assessment.

ANPRM Publication Date

The ANPRM was posted on the *Federal Register's* website on Thursday, December 15, 2016, at 8:45 a.m. and published in the *Federal Register* on Friday, December 16, 2016. The ANPRM

~~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.~~

was published in a separate Part 3 of the *Federal Register* together with the Notice of Proposed Rulemaking (NPRM) on Security Training for Surface Transportation Employees.

Next Significant Actions

The ANPRM public comment period will close on February 15, 2016, 60 days after the date of publication in the *Federal Register*. Thereafter, TSA will draft the NPRM, including proposed rule text, preamble, and Regulatory Impact Analysis, and will continue to prioritize this rulemaking.

Outside Interest

Members of Congress (primarily Senators Booker and Blumenthal) have expressed interest regarding the status of the 9/11 Act surface rulemakings at hearings and through correspondence with TSA and DHS.

In addition, the DHS Office of Inspector General (OIG) recently conducted an audit and issued a report on May 13, 2016, titled "TSA Oversight of National Passenger Rail System Security." The report included two recommendations: (1) the Administrator should ensure that TSA develops and adheres to a detailed formal milestone plan to deliver the outstanding 9/11 Act rulemakings to DHS; and (2) that DHS OGC coordinate with OMB to expedite implementation of the remaining 9/11 Act requirements. Both recommendations remain open.

While we do not anticipate any litigation risk associated with this proposed rule, Congress and stakeholders may raise concerns regarding the narrowed scope of the proposed rule's applicability (the proposed rule is limited to higher risk entities).

~~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 Presidential Transition Landing Team Questions for TSA

203. Provide the publically available white paper on FAMS.

Response: We do not have a publically available white paper on FAMS. We would be happy to set up a separate classified briefing upon request.

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 elect President- 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 Presidential Transition Landing Team Questions for TSA

204. Provide the polygraph washout rate for FAMS candidates.

Response: Since commencing the FAMS Law Enforcement Pre-Employment polygraph examination on May 1, 2016, thirty-two (32) percent of FAM candidates were not able to continue in the application process due to their polygraph results.

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 elect President- 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.

TSA ROADMAP

Transportation Security Administration

Issued December 2016

Transportation Security Administration

December 2016

I am pleased to present the TSA Roadmap. This Roadmap is intended to tell the story of the Transportation Security Administration over the course of my tenure as Administrator. In doing so, this brief document will assist readers in understanding the challenges TSA faced, what actions we took to address them, what is on the horizon for the Agency, and, perhaps most importantly, what we must focus on to position TSA for long-term, sustainable excellence.

What I ultimately hope to convey is the urgent need to sustain momentum in our comprehensive efforts to transform TSA into a next-generation counterterrorism organization. TSA is a proud security agency that has changed dramatically since I arrived 18 months ago. That is because we aggressively examined and questioned ourselves, reaffirmed our identity and true security mission, reconnected and collaborated with the industries and the public we serve, and hard-wired innovation into a reinvented entrepreneurial culture.

To be sure, TSA is not yet where it needs to be, but we have charted a way ahead. Indeed, I strongly believe that our efforts to date have put TSA on the path to successfully meeting any challenge, no matter how unfamiliar or potent. Specifically, human capital, training, acquisitions, innovation, operations, and partnerships are the "levers of transformation" for delivering mission success now and into the future.

TSA is charged with a critical mission: protecting the nation's transportation systems to ensure freedom of movement for people and commerce. This sacred trust means that security effectiveness must remain the Agency's top priority. By advancing the initiatives described in the Roadmap, TSA will continue on the trajectory needed to effectively counter threats from a creative, determined, and adaptive enemy.

Sincerely,

Peter V. Neffenger
Administrator

PURPOSE

This Roadmap is intended to tell the story of the Transportation Security Administration over the course of my tenure as Administrator as well as to assist senior government leaders in understanding the strategic U.S. transportation security environment and current TSA initiatives. In doing so, the document will recount recent history, outline what we have done and why, chart where I believe we are headed, and recommend what we need to focus on to get there.

WHAT WE FACED:

The Strategic Environment

When I came to TSA in summer 2015, I found an organization staffed by capable, dedicated professionals who routinely put the interests of the agency, and the nation, before their own. However, I also found an organization reeling from the disturbing results of covert testing by the Department of Homeland Security's Office of the Inspector General (DHS OIG) of passenger screening operations. The results had been leaked to the media and called into question our ability to conduct our fundamental mission to protect the aviation system. This also caused the agency and its people considerable public embarrassment and ridicule. TSA was in trouble, under scrutiny, and in desperate need of change. To make matters more complicated, TSA faced a constellation of environmental barriers to success, internally and externally.

Evolving Threat Environment

While we remain confident that we can protect against the kind of attack that occurred on 9/11, today's shifting threat environment is, in many ways, more dynamic, profound, and complex than ever before, and certainly more so than the one we faced when TSA was established. At that time, for example, our detection efforts were focused on guns, knives, and commercial and military grade explosives. Liquid and homemade explosives were still nascent threats. Now, TSA must address a much wider, more lethal, and more complex range of explosives, and these can be presented to us in a multitude of configurations and threat pathways. Moreover, the threat has expanded over the airwaves and into cyberspace. Today, we face a diffuse and dispersed enemy that masterfully manipulates communications and media, not only to direct attacks but also to inspire, enable, and claim credit for them.

Not only has the threat environment changed from a world of terrorist-directed attacks to one that includes the threat of terrorist-inspired/enabled attacks, the enemy is now significantly compressing the timeframe from plot to action. Employing different combinations of new actors, previously used methods, and novel tactics, the terrorist diaspora is leaving less time, and hence fewer opportunities, for their increasingly sophisticated efforts to be thwarted.

What has not changed is that terrorists still consider airlines and airports high-value targets. The U.S. air transportation system, especially passenger airplanes, remain a primary target of every global terrorist network. That has not changed since before 9/11 and will define the threat environment for years, maybe decades, to come.

Workforce Levels

From 2011 to 2015, TSA had experienced a steady, year-over-year reduction in its front-line workforce. Like other federal agencies, we faced an austere budget climate. TSA's reduction was perhaps exacerbated by the initial miscalculation that TSA Pre✓® expansion could be a viable substitute for manpower. Coupled with forecasts of year-over-year passenger volume growth for the foreseeable future, the decreased capacity base was, in retrospect, a perfect storm waiting to happen.

FY11 FY12 FY13 FY14 FY15 FY16

Stakeholder Relations

Our relationships with critical stakeholders were in dire need of attention. The traveling public saw TSA as a necessary nuisance to be endured and tolerated. Many in Congress viewed TSA as an unfixable bureaucracy with an unachievable mission. Industry looked at TSA and saw an obstacle to business success and another factor that contributed to travelers' frustration, frequently putting TSA at odds with transportation partners. Regrettably, we were working at cross-purposes when we should have been working closely together in pursuit of a shared goal: the security of our nation's transportation system. Other stakeholders greeted TSA efforts with tepid support or indifference. That lukewarm reception, however, could quickly boil over to anger when TSA was portrayed as violating the public trust.

WHAT WE FOUND:

The Operational Environment

As an agency, TSA had become inured to the drumbeat of complaints and criticisms from the public, media, Congress, and industry. We had come to internalize that vilification and accept that being disliked was part and parcel of our job. That perspective led, in turn, to an ossification of how we conducted our business. Plagued by poor perception from our stakeholder community, TSA took comfort in rigid compliance with standard procedures. We were performing a public service under constant scrutiny, with the ever-looming threat of any missteps being plastered across tomorrow's front page. Under such bombardment, sticking with "standard" seemed to be the safest port in the storm and makes the continued dedication of our people all the more commendable. Our stakeholders seemed so sure of the intractability of TSA's problems that they were skeptical of and unreceptive to any proposals to "transform" what many among them perceived to be a hopelessly broken agency. Then came the leaked DHS OIG report.

Identity Crisis

In May 2015, the DHS OIG notified TSA that it had conducted covert testing of airport checkpoints and, in several attempts, successfully transported explosives and firearms into sterile areas.

TSA's brand identity was largely dictated by its visual presence at airports despite our active engagement behind the scenes with intelligence and federal air marshals, for instance, and our engagement with local and state officials in surface transportation. We are, by far, the most visible and ubiquitous retail face of government, and the leaked DHS OIG report appeared to deal irreparable damage.

But the report also prompted us to ask the kind of difficult soul-searching questions that are necessary for a struggling organization to right itself. What is TSA at its core? What do we stand for and how does that affect our relationships with the traveling public, our partners, and environment? What should our future look like? Those questions forced a hard look at the status quo, a close reexamination of our operations and mission support functions, and perhaps most importantly, a deliberate and systematic focus on developing a new agency culture.

Amidst the turmoil of the report, TSA senior leadership quickly recognized that our people, while understandably demoralized by the report's findings, have never failed to do what was asked of them. The problem, as we discovered, had been what was asked, how we asked it, and how we defined our mission. We were directing our people to view the balance between three drivers – security effectiveness, operational efficiency, and the traveler experience – as a zero-sum game, a static "pie" of determinate size and proportions. Then we asked them to line up behind one driver at the expense of the others.

As a result, we lost sight of our primary mission – security – which unwittingly pitted us against the very stakeholders from whom we needed help. TSA repeatedly was caught on its heels, reacting to crisis after crisis, seemingly stuck trying to catch up with the latest negative headline. We were risk averse, tentative, and defensive. We needed to pause, take a step back, and see the big picture. We had to adopt a decidedly systematic approach, an across-the-board reinvention, and rediscover ourselves as an agency and our sacred trust as protectors of the nation's transportation system.

Process Gaps

Stove-piped and outdated processes compounded the aforementioned challenges. TSA was, of course, stood up in urgent response to a crisis. Functions grew or were added as needed, while organizational positioning and effective internal processes were sacrificed, at least temporarily, for expediency. But a decade and a half later we found that the organizational structure that was built reactively – and to react – was taken for granted and needed reexamination.

Following are some examples of where we identified the existing structure could be improved:

TSA's acquisition programs historically have existed in individual program offices stationed across many of the 18 lines of business within the agency. In 2015, this decentralized approach was identified as an enterprise risk to TSA's mission. As a result, we conducted a review of TSA's acquisition programs in concert with the independent Defense Acquisition University, resulting in recommendations for organizational improvements and process efficiencies that would mitigate this risk.

With a diverse workforce geographically dispersed across hundreds of locations employing a variety of local practices, TSA has faced considerable challenges in instituting effective enterprise human capital management. While the Office of Human Capital (OHC) directs human resources policies and procedures, human resources staff and administrative officers in the 439 TSA field offices are currently directed by and report to the agency's myriad operational components. Over time, this has created many inconsistencies in human capital delivery and communications in all areas, from human resources operations to employee development and engagement.

Furthermore, TSA did not have a consolidated, coordinated approach to human capital management. Many of the agency's critical human resources functions and operations had been outsourced to a large, multiple-year contract which began at the end of 2008 and will be coming to a close in early 2017. In-depth reviews of this contract reveal a deep need to reassess the agency's approach to human capital operations and develop a strategy that will reduce risk, increase efficiency and effectiveness, be more responsive to workforce needs, and provide improved adaptability to TSA's evolving requirements.

Workforce training and development were highly decentralized with primary responsibilities falling to OHC for leadership and other soft-skills training, and to the Office of Security Operations (OSO) for Transportation Security Officer (TSO) screening workforce technical training. Most other TSA Offices managed their own training initiatives. The Office of Training and Workforce Engagement (OTWE), now renamed the Office of Training and Development (OTD), was created in November 2011. This was an initial step to consolidate some of the training functions within the agency, but much training was still managed and executed in a decentralized manner. For instance, while the TSO technical training syllabus was prepared by OTWE/OTD, the actual training delivery was performed by decentralized and distributed trainers attached to individual airports across the country. This led to inconsistent and variable training with little oversight, tracking, or outcome-based measures of success.

These and other examples depict an organization subject to centrifugal forces that disconnected it from its primary mission.

WHAT WE DID:

The Actions Taken

On the heels of the DHS OIG report, we conducted an in-depth root-cause analysis that yielded valuable insights into the underlying, multidimensional reasons for the covert testing failures. A number of systemic factors had influenced the conduct of screening operations, among these, disproportionately prioritizing screening speed over security effectiveness. Indeed, across the enterprise, leaders' and officers' organizational behavior emphasized efficiency outcomes (defined as short lines), with pressure to clear passengers rather than diligently resolving alarms. Many of the challenges confronting TSA were interwoven and mutually reinforcing.

Focus on Effectiveness

We shifted our strategy and resources to prioritize effectiveness. Among other efforts:

- We conducted a rolling training stand-down across the entire workforce in August and September 2015, eight hours at a time, to retrain our full workforce (including leadership at all levels) to explain in detail the nature of our failures, to better understand the capabilities and limitations of our equipment, and ultimately to refocus on security effectiveness.
- We learned that we had to manage the approaches to airport checkpoints as a separate security element, and not as an added burden to our TSOs as they performed their demanding and complex duties to identify potential threats and prevent prohibited items from making it through screening.

We established and instituted new performance metrics, emphasizing system and people readiness over wait times at airport checkpoints.

We redefined our value proposition as a national security counterterrorism agency, which meant we needed to radically alter our relationship with our environment and its many actors, because only with close and consistent collaboration with our partners could we follow through on that value proposition.

An outstanding example of what can be accomplished through public/private partnership was the establishment of the Incident Command Center (ICC) to help address air passenger volume growth, especially during the busy summer travel season. Using nationally accepted incident management concepts, the ICC closely tracked daily screening operations and reassigned officers, canine resources, the National Deployment Force, and other resources accordingly to meet mission demands in advance of predicted passenger volume. These efforts improved our ability to deploy the resources we needed in the most efficient and effective manner possible to screen the record number of passengers transiting through our nation's airports last summer.

Industry representatives, including airports and airlines, Airports Council International – North America (ACI-NA), the American Association of Airport Executives (AAAE), and Airlines for America (A4A), have actively participated in the daily planning calls. The ICC became a permanent operations hub and was rechristened as the Airport Operations Center (AOC) after Labor Day, thus signifying our long-term commitment to this initiative. Indeed, our partners have come to rely on the comprehensive reports issued by the AOC, such as the Hot Spot reports, the daily Situation reports, and the Movement and Volume reports. Also, having industry and TSA on the phone together understanding one another's issues and concerns has significantly enhanced communications and cooperation at the operational level. Lastly, the TSA Aviation Security Advisory Committee (ASAC) continues to provide significant industry recommendations to the agency on several matters, including insider threat, air cargo, general aviation, and international aviation.

Resource to Meet Demand

With a renewed focus on identity grounded in security effectiveness, we had to reverse the recent trend of workforce reductions. To that end and working with a supportive Congress, TSA halted the planned reduction of 1,660 officers in Fiscal Year 2016, expedited the hiring of over 1,300 new officers, converted more than 2,000 part-time officers to full-time status, augmented and redistributed canine team assets, and added nearly 800,000 hours of authorized overtime. In close partnership with Congress, we secured support for three FY 2016 budget reprogramming requests, totaling $118 million, to mitigate vulnerabilities, address passenger volume growth, and improve effectiveness. These reprogramming actions allowed TSA to procure nearly 150 new Advanced Imaging Technology machines for deployment to smaller airports, replace almost 1,200 Explosives Trace Detection units with more capable machines, and accelerate support for Technology Infrastructure Modernization, which provides enrollment, vetting, and credentialing services for millions of people across multiple transportation sector populations.

Transform the Organization

It led to changing the way we think about, prepare for, and execute our complex mission in an extremely dynamic and challenging threat environment. Even as we have tackled the root causes of the DHS OIG report's findings and successfully addressed the headline-grabbing wait times in the face of record air travel passenger volume, we have kept our focus on who we are and how we need to transform to meet future threats. With this in mind, our renewed

Airport Operations Center,
real time tracking of passengers
airport by airport.

commitment to our identity surfaced three very simple guiding principles that were codified in my Administrator's Intent published in January 2016:

Focus on Mission

Invest in People

Commit to Excellence

To advance these principles, we directed our efforts toward training, acquisitions, and innovation delivery.

In addition, TSA recently contracted RAND to complete an additional assessment of the effective integration of our leadership team and the maturity of the TSA enterprise. As part of the process, RAND independently validated the principles driving our organizational change.

Transform the Organization: Training and Education

As noted above, in July 2015, TSA did not have a centralized, consistent, and coordinated approach to training. Training is the foundation of mission success and a powerful tool in galvanizing and leading change. It provides consistency, develops a common culture, instills core values, improves morale, and it raises performance. To that end, we promulgated the TSA Training and Development Roadmap, which incorporates risk-based concepts and intelligence-driven principles to address root causes by pursuing five specific lines of effort: 1.) new hire training, 2.) mission-focused leadership training and development, 3.) training standards and certification, 4.) recurrent training, and 5.) training requirements.

In January 2016, we established the first-ever full-time TSA Academy at the Federal Law Enforcement Training Centers (FLETC) in Glynco, Georgia. We inaugurated this Academy by sending all new-hire Transportation Security Officers to a fully redesigned basic training course beginning on January 1, 2016. We eliminated the inconsistent and uncoordinated delivery of training scattered across some 75 airports by establishing a shared experience of training alongside fellow officers from around the country to build morale, create a new culture, and ensure a collective understanding of TSA's mission and operations. Since January 2016, TSA has graduated over 6,100 new TSOs, roughly 14 percent of our workforce, spread across the network of more than 450 airports. In FY 2017, we expect to train more than 8,000 new officers at the TSA Academy.

We also established the first-ever executive education development program in the history of TSA. In 2016, every senior executive attended the National Preparedness Leadership Initiative (NPLI) course, a national education program specifically designed for developing government leaders who must be prepared to lead in complexity and respond to crisis. Incumbent TSES employees will be required to complete specified mission-focused professional development every three to five years to reinforce and maintain leadership competencies. The recurrent training will consist of a one-week in-residence session and executive coaching for TSES leaders.

NPLI for TSES

5

cohorts completed

130

participants

TSO Basic

5947

graduates in FY16

264

classes

Transform the Organization: Acquisitions and PPBE

In November 2015, the Defense Acquisition University began an independent analysis of our acquisition processes and organization, identifying reforms that will provide sound governance and constrain program slippage, cost overruns, and requirements evolution. By implementing the study's recommendations, TSA is consolidating acquisition programs into the Component Acquisition Executive organization and potentially saving millions of dollars through effective requirements generation and acquisition discipline. Related to that effort, we are building a new Program Planning, Budgeting, and Execution (PPBE) process to reform oversight and governance, and to link long-term mission needs to our budget priorities. The output of the PPBE process will be a risk-based, defendable, and executable multi-year plan for TSA to submit to DHS. Our reprogramming submissions this year, and the budget we expect to present next year are a direct outcome of this new process.

Transform the Organization: Innovation Task Force

In order to ensure that TSA evolves to stay ahead of a dynamic threat environment and is able to accommodate and respond to future circumstances, we established an Innovation Task Force, which provides industry partners, including airlines, airports, surface mode operators, and technology manufacturers, with a platform to develop innovative solutions as we envision transportation security of the future, allowing us to partner with industry to demonstrate emerging technologies in an operational environment. Part of this effort is to model the entire system to emphasize effectiveness by identifying opportunities for improvement, closing process gaps, and addressing emerging threats.

Automated Screening Lanes

CT Scanning Accessible Property

Biometric Identity Authentication

WHAT WE CONSIDERED IMPORTANT:
Levers of Transformation

Even as we effectively executed our plan to address the short-term issues, sustaining the momentum for long-term success is critical to our ongoing commitment to excellence. The agency had been caught in a web of colliding systemic problems.

With nearly 6,000 regulated corporate facilities, over 22,000 regulated stations, and more than 88,000 inspections across all transportation modes in FY 2016, we set the guidelines and then actively participate in delivering on them alongside our transportation security partners.

Because the sources of difficulty for the agency were interconnected, we had to conceive and implement a set of clear priorities that were likewise interdependent to reverse this dangerous course. Between the internal challenges posed by the operational environment and the external pressures exerted by the strategic environment outlined above, we had to start from the ground up in order to chart a better way forward that gave direction and purpose to our investments – in our people, in our processes, and in our technologies.

Enablers of Mission Success

In leading the agency, we have pursued a number of strategic pathways to guide our collective efforts by reengineering enterprise-wide behavior at TSA. Thinking about what constitutes enterprise behavior, we categorized our actions into the following separate groups:

- Human Capital
- Training and Education

Acquisitions/Program Planning, Budgeting, and Execution (PPBE)

Innovation

Operations/Mission Support

Partnerships

These functions tie directly to our foundation: people. Human capital identifies, recruits, and retains the right people. Training provides our people with the requisite skills and knowledge to succeed in their jobs. Resource allocation using disciplined acquisition and PPBE processes ensures we have the appropriate staffing levels and the right capabilities so our people can do their jobs. Innovation affords our people opportunities to challenge and reform processes and policies in addition to introduce novel solutions to further enhance our mission delivery. Operations put our people in the right place at the right time doing the right things. Finally, partnerships across the transportation enterprise are essential to achieving genuine collaboration that empowers our people within the multi-actor security continuum. These are the enablers of mission success.

In order to solidify the gains made and lay the foundation for sustainable, high performance, we once again returned to the business functions that directly impact our greatest resource. If we are to become the world's preeminent transportation counterterrorism organization, we have to field the best capabilities, provide world-class training, and retain the organizational knowledge and skills to stay ahead of an entrepreneurial, adaptable, and creative enemy.

Entrepreneurial Culture

At the heart of TSA's transformation is the introduction of an entrepreneurial culture that informs and infuses every aspect of our organization. Disseminating this mindset has prompted a radical reimagining of our operations and support functions. While a profound departure from our traditional way of doing business, our entrepreneurial approach already has yielded some "early wins" such as the TSA Academy, the Innovation Task Force, and reinvigorated partnerships with our transportation industry stakeholders. It is imperative that we continue on this path.

Push bin forward 4
Push bin forward
Put items and bags into bin
Place bin here
Push bin forward 4
4 Push bin forward
3 Put items and bags into bin
2 Place bin here

WHAT IS ON THE HORIZON:
Short-Term Next Steps

Transforming a large organization, especially a government agency, is no easy task. Both the strategic environment and the operational environment influence an organization's willingness and ability to execute far-reaching change. Moreover, we have varying levels of direct control over the factors that contribute to organizational transformation. External indifference, internal resistance, and budgetary constraints are among the many issues that can and do alter the trajectory an agency sets for itself. For that reason, the strategic focus areas –

the importance of this point cannot be overstated.

Human Capital Management Strategy

Because the agency stood up in crisis, widespread contractor support was required to meet the necessarily ambitious timeframes. Only with the assistance of contractors, especially in our human resources functions, could TSA ramp up from scratch to the neighborhood of 50,000 employees in six months. However, this became the longstanding way we did business rather than merely a temporary measure to get the agency on its feet. In order to evolve the human capital enterprise, address the human capital challenges of tomorrow head on, and thereby further the broader TSA transformation, we need to strike the appropriate balance between contractors and internal management support of our human capital strategy going forward.

We will fully develop and implement the HR Enterprise Solution. This will centralize and standardize human capital functions within TSA, aligning human resources roles across the enterprise and streamlining operations by consolidating management control. Also, TSA will sunset its current single-source human resources contract and

combine the strategic insourcing and outsourcing of the agency's enterprise-level human resources services in order to minimize risk and increase effectiveness. In doing so, we will ensure greater transparency and promote confidence in our human capital process and procedures by providing our customer with service-level standards and metrics on service delivery.

The forthcoming Human Capital Strategic Plan will provide human capital strategies to acquire a highly qualified and diverse workforce; foster an agency culture of excellence through inclusion and engagement; and achieve human resources operational excellence. The plan will address fundamental recruitment, development, promotion, assignment, and retention issues by providing a structured approach toward how we invest in our people, incorporating the framework for human capital policies, programs, and practices to ensure that we are investing in our people via a common vision.

Training and Education

Training and development are foundational to organizational culture, and are therefore instrumental to radically reshaping an agency. In addition, training connects people to the mission and inculcates mission focus, which reinforces the message of how we define ourselves. We will institutionalize the TSA Training and Development Roadmap to focus on new hire training, mission-focused leadership training and development, training standards and certification, recurrent training, and training requirements across the spectrum of agency populations and throughout the entire career progression.

TSA and FLETC are contracting for Architecture and Engineering design of a state-of-the art TSO training facility at FLETC. We are continuing efforts to centralize all training management under OTD to ensure effective oversight of all workforce training. Moreover, TSA is working to acquire Federal Law Enforcement Training Accreditation (FLETA) for the TSA Academy and its basic training courses. This accreditation will give TSA official recognition in the federal law enforcement community for its commitment to providing quality training. Anticipated to be at full operational capability in FY 2017, the TSA Academy expects to train 8,000 front-line employees next fiscal year.

Regarding mission-focused leadership training, as employees are promoted to mid-level positions and above, TSA will leverage partnerships with Institutions of Higher Education (IHEs) to provide mandatory leadership training starting in January 2017. The intent will be to enhance leadership skills that align with the Office of Personnel Management's (OPM) Executive Core Qualifications (ECQs), and to promote continuity of themes, expectations, and lexicon along the entire leadership training progression.

TSA will partner with accredited IHEs to develop and deliver a mandatory program for mid-level and senior level employees within six months of promotion (approximately 190 and 90, respectively, per year) that will provide a multi-disciplinary approach that emphasizes leadership in a risk-based security environment and cultivates their OPM ECQs. In addition, within six months of promotion, all mid-level employees (approximately 15 per year) will be required to attend the Federal Executive Institute's (FEI) Leadership for a Democratic Society course in partnership with OPM.

All Federal Security Directors (FSDs) and Deputy FSDs (DFSDs) will be required to attend the FSD Training Course within six months of appointment as well as recurrent training annually thereafter. This phased curriculum incorporates leadership principles, incident and risk management, operational and performance management, and stakeholder engagement and planning. The courses will be delivered at TSA headquarters, as many of the modules require sustained personal engagement with the Administrator and senior leadership team.

Acquisitions/PPBE

Reengineering acquisitions and instituting a disciplined PPBE process offer a systematic way to provide the capabilities where and when they are needed. Building flexibility and responsiveness into the system will pay dividends for hiring, training, and equipping our workforce with the right tools at the right time to perform their duties.

To support effective acquisitions and procurements, we will continue to examine each acquisition strategy to ensure that an alternative approach would not provide lower programmatic risk. We will continue to align resources and requirements to mission needs, thereby optimizing future operations. As we implement the Acquisition Reform Task Force strategy, we will align our strategic goals based on past lessons learned to modify and further develop future objectives.

Furthermore, we need to ensure that acquisition and contracting processes are flexible and function optimally to ensure that mission critical capabilities are fielded in a timely manner. To more effectively provide the front-line with mission critical support at a cost-efficient price, TSA needs to build the Office of Acquisition Program Management and the Office of Contracts and Procurement, and establish a culture of service, expertise, and engagement therein.

For a more disciplined PPBE process, TSA will conduct the FY 2019-2023 TSA Resource Allocation Program review to provide a common understanding across Program Evaluation Groups (PEGs) of each TSA program, and recommend a Core (non-discretionary) funding profile to leadership in advance of generating trade space. In addition, we will implement the Budgeting Programming and Resource System (BPARS) as well as the Decision Lens Tool to allow for fact-based discussion of various budget choices.

TSA's budget request and mid-term planning reflect the structural adjustments that are necessary. TSA's future budget requests will support Department priorities while seeking structural adjustments needed to resource TSA to keep pace with evolving threats and improve the effectiveness of the screening system, posture for continual passenger growth, and close passenger screening capability gaps by investing in detection technology equipment, the number of canine teams, cyber security for mission-essential systems, and cargo screening capabilities.

Innovation

The Innovation Task Force represents a formal, repeatable mechanism for fundamentally changing the entire system, even as we commit to excellence in our current operations. It allows us to think deeply about tomorrow's promises while effectively and efficiently addressing today's perils.

For the external environment, it serves as an important "receptacle" for and connection node with our private sector partners to introduce innovative solutions into the security enterprise and allow them to gestate, with the eventual goal of deploying them across the agency once they are ready.

To prioritize solution development and risk-based capabilities, TSA has aligned its efforts around four themes outlined in the TSA Strategic Five-Year Technology Investment Plan:

- Integrating Principles of Risk-Based Security in Capabilities, Processes, and Technologies
- Enhancing Core Mission Delivery by Focusing on System of Systems
- Streamlining Acquisitions, Requirements, and Test and Evaluation Processes
- Increasing Transparency in Engagement with Stakeholders to Enable Innovation

Continuing with the theme of culture change, we are working diligently to "hardwire" innovation into the way we think and what we do, inculcating an entrepreneurial mindset throughout the organization. Innovation Task Force solutions

may cover a breadth of topics, from policy and process changes to training solutions to new detection technologies, all with the goal of enhancing security effectiveness, while improving efficiency and the passenger experience "from reservation to destination." TSA is building on its successes with the Innovation Task Force by developing an executable strategic plan that details goals, objectives, timelines, deliverables, and transition options for solutions.

Building a true enterprise solution requires that multiple TSA offices work collaboratively to interconnect Transportation Security Equipment (TSE), thereby enabling the agency to centrally track and harmonize TSE settings, remotely monitor and maintain TSE availability, transfer passenger risk information directly to the checkpoint, and automate data collection processes. Future efforts include exploring third-party sensors connection to the TSA network and use of advanced software to automatically identify potential internal/external threats in real time, with the goal of building a reservation-to-destination view of airport operations. The goal is to modernize an otherwise analog operation and support infrastructure.

As the frontiers of the threat environment expand into the virtual world and adversaries vie for access to valuable sensitive information, we will continue monitoring cyber vulnerabilities, supporting at-risk systems, leveraging TSA-wide procurements, consolidating data centers and moving IT systems to the cloud, and creating a functionally aligned organizational structure.

Operations/Mission Support

In 2016 we established a new Chief of Operations position to integrate the various operating programs of TSA, which span several functions from airport security and federal air marshals to multimodal transport and pipelines. Taking a fresh look at operations empowered us to focus on and deliver mission beyond "how we have always done things." TSA is truly the retail face of government. Who we are matters to over 2 million travelers at airports, 28 million passenger rail riders, 1.2 million trucking companies, 3,000 privately owned pipeline companies, 106 million ferry passengers, and 11 million cruise ship passengers with whom we interact each day through our integration with state and local authorities. Our operations represent the points of interface with the traveling public, industry partners, and congressional overseers. They shape stakeholder and public perceptions. So the Chief of Operations position was instrumental in coordinating across TSA offices to address the surge in travelers in summer 2016, including the launch of the cross-office ICC (now AOC).

In order to unify the many efforts across the agency and align with traditional management theory on span of control, we also established a Chief of Mission Support function, which integrates enterprise-wide support to operations. The new position will drive unity of effort and enterprise approaches to human resources, acquisition and procurement, training, logistics and other important mission support activities. This initiative is a critical piece of our effort to establish long-term stability and unity in the leadership structure of TSA. As a result, key decision making, communication, and oversight functions are retained as direct reports to the Administrator and Deputy Administrator. Following the arrival of the Chief of Mission Support, charters for new governance mechanisms will be instituted that will facilitate timely cross-office decisions.

Our homeland security depends on strong security regimes across the world. So we must continue to advance global security standards, ensuring their consistent application and enforcement in addition to an international audit regime that improves security at overseas last-point-of-departure airports. We are applying lessons from our experience in connecting processes, people, and organizations to make the system better. With the recent unanimous adoption of United Nations Security Council Resolution 2309, we have an unprecedented opportunity to realize a global aviation security system that ensures that security will become as much a part of aviation as safety has been since the industry's birth.

We must advance the design and implementation of enterprise metrics that incentivize and measure progress towards the desired outcomes. Ways to measure results in the critical support functions need to be tightly integrated with how

operations are executed. System performance, officer readiness and performance, "time-to-market," staff attrition, detection rates, leadership engagements, cost savings, system readiness, wait times, and employee surveys are among the many various qualitative and quantitative data that could be collected, tracked, and cross-referenced. But they ultimately need to be tied to the well-being of our people and their capacity to grow and advance the mission.

Partnerships

TSA has broad authority to prescribe regulations, standards, and procedures; issue orders and security directives in response to threats; conduct investigations; and enter into cooperative arrangements. However, we now see ourselves as a part – a critical part – of the transportation security continuum, and being part of that continuum, TSA must rely on trusted partners to accomplish the mission. That is why TSA is entering a new era for partnerships.

We want to leverage private-public partnerships to create an enhanced security environment through collaborative engagement with all stakeholders. For example, starting in fall 2016 and in partnership with DHS Infrastructure Protection, TSA co-hosted a series of public area security summits to counter evolving tactics deployed by transnational terrorist organizations. The goal of these summits is to establish a national-level framework on how we can collectively counter threats to public areas. The participation of both government and industry executives provided a unique opportunity to not only leverage their expertise, but to make everyone an investor in the national framework. By bringing this group together, we realized that we had all the authorities needed, multiple funding streams to take advantage of, and the world's leading experts. TSA intends to continue fostering collaborative partnerships with all stakeholders as we continue to deter, detect, and disrupt emerging threats and plan for public security in all transportation arenas.

WHAT WE ASPIRE TO BECOME:
The Envisioned State

The only way to defeat such an enemy is to continually grow and reinvent. TSA must infuse an entrepreneurial spirit into every facet of its operations and make it a way of life. To achieve and perpetuate that state of mind, we need to address three principal areas: organizational change, processes, and leadership.

For TSA, targeting the underlying levers of transformation has enabled organizational change. However, sustaining the self-critical outlook that drives entrepreneurialism also requires the right processes in place and firm commitment from leadership enterprise-wide. The realignment of requirements to a dedicated Office of Requirements and Capabilities Analysis, the creation of the Chief of Performance and Enterprise Risk position, and decoupling acquisitions and procurement into an Office of Acquisition Program Management and Head Contracting Authority are important steps to ensuring processes are efficient, responsive, and mission-focused. Furthermore, leadership development has remained an agency priority. NPLI is the first of a series of recurring training initiatives for our most seasoned executives, but learning opportunities abound across an employee's entire career progression. With comprehensive training requirements, leaders across the organization will be equipped with a shared vocabulary, set of expectations, and cultural emphasis on self-critical reinvention.

Security Culture

Safety is already ingrained into the transportation culture as second nature, from the corpus of regulations and inspection checklists to pre-flight routines and the passenger reflex to fasten seatbelts. At this point, the same cannot be said about security, which routinely has been regarded as an appendage and a course of action that "someone else" handled. We need to weave security into the fabric of aviation and the broader transportation industry as well – a holistic, ecosystem view that builds a culture of security and integrates all security elements: checkpoint, landside, perimeter, passenger, workers, access control to secure areas, and so forth.

We will continue to invest in new technology to advance security effectiveness and improve the traveler experience, envisioning a future where screening matches the speed of life. To support that vision, our financial, acquisition, and procurement functions will be forward-thinking to ensure steady-state resources with the anticipated 2 to 7 percent air passenger volume growth annually for the next three years.

TSA must and will think and act beyond boundaries, both in a literal and figurative sense, as we build an international audit regime, hardwire innovation into our entrepreneurial culture, institutionalize investment in training and leadership development, evolve the PPBE process, and genuinely collaborate with stakeholders to meet the diverse needs of the traveling public.

Security Ecosystem

The mutually reinforcing interdependence of stakeholders, data, processes, technology – the system of systems – requires an organization that is dynamic, effects-based, intelligence-driven, and adaptable.

TSA will continuously achieve excellence in developing and deploying innovative processes to recruit, hire, inspire, develop, engage, and retain high-quality candidates that meet mission needs. This will be supported through the HR Enterprise Solution strategy as well as a robustly enhanced HR operational capacity via the new service delivery model.

We will continue to upgrade and modernize mission-supporting IT infrastructure and applications. Our goals include focusing on our security mission while concurrently enhancing and supporting the traveler's reservation-to-destination experience, using technologies such as business intelligence and machine learning to inform and improve risk-based decision-making across the enterprise, proactively protecting IT services by continuing to make cybersecurity a mission enabler rather than an afterthought, and evolving the IT workforce to meet the challenges associated with managing new technologies and development methodologies.

Counterterrorism and Security Professional

A recurring theme in this Roadmap – and TSA's history as an agency – has been change: momentum, dynamism, evolution, and transformation. That turbulence was sometimes triggered by an external event and other times as part of a deliberate plan. Yet the one constant has been the tireless dedication of our workforce. The workforce has always done what was asked of them. They have reacted swiftly to measures put in place to evolve the agency. They are stewards of our future, the actors that make real and lasting change possible. In the tempest of competing priorities, the weathervane should ultimately point to our people and how to improve their performance and job satisfaction. They are the reservoir of organizational knowledge as well as the ultimate drivers of mission success.

The challenge is to marshal that resource and redirect its energies to the right objectives. The future we envision will be people-focused and people-driven. Losing one's identity can be significantly easier and quicker than rediscovering it. For that reason, we need to remain vigilant and focused on connecting our people to the mission. We had already undergone a seismic shift in how we viewed ourselves; we cannot afford to be complacent and regress.

To effect enduring change, TSA must firmly establish the TSA Academy as the Center of Excellence (COE) for national transportation security training and development. The academy will represent the global TSA training and educational enterprise with its overarching management structure located at FLETC and associate training facilities in Atlantic City, NJ and San Antonio, TX. Training and education courses will span the breadth of TSA's multi-modal mission. This new training enterprise will revolutionize the provision and oversight of TSA training, improve the performance of the TSA workforce and foster a greater sense of duty and purpose among employees. TSA will be a true learning organization that is not only conscientious in measuring performance, but also people-focused in how the results are applied to make TSA better.

To realize the potential of the agency, we must envision the future state of our most important of resources – our people. To that end, we will invest in every employee to ensure they possess the competencies of a counterterrorism and security professional: aware, proficient, and results-driven. These attributes enable the agency to accomplish a range of missions while operating in a challenging and changing transportation security environment. Awareness requires every TSA employee to understand the threat, use intelligence to inform daily operations, be knowledgeable of the air, surface, and pipeline operating environments, and know the capabilities of the tools, systems, and equipment we employ. Proficiency requires our people to master the skills required of their mission area or function, from screening and inspection, to intelligence analysis and mission support operations. A results-driven workforce sustains high performance in the execution of core mission tasks. As counterterrorism and security professionals, our people will demonstrate the knowledge, skills, abilities, and values to consistently deliver excellence in mission priorities, and continuously improve themselves to add value in the agency's mission to protect transportation. They will lead, enable, and drive the security ecosystem of the future.

FAMS

TSA K9
ICE

WHAT THE FUTURE HOLDS:
Delivering Mission Success

The activities described herein only scratch the surface of what TSA undertakes every day. The breadth and depth of the efforts across the enterprise are staggering, and the people behind each one contribute to mission success in unique and meaningful ways. The intent of this Roadmap is to tell a story about the lessons we have learned over the past 18 months, and in the process, provide a useful management tool. By recounting our recent challenges, describing how we addressed them, and sharing some thoughts about the path ahead, I hope to have set a trajectory for sustained high performance and establish the building blocks to help TSA get to the destination.

Where we came from 18 months ago seems like a far cry from where we are today. However, the path from then to now was charted deliberately, with specific guiding principles informing every step of the journey. To be sure, we are not yet where we need to be, but we know where we are going. TSA is a good and proud agency that has changed dramatically over the past year and a half. We have accomplished that by aggressively examining and questioning ourselves, by reaffirming our identity, by understanding our true mission, by reconnecting and collaborating with the industries and the public we serve and by becoming innovative and entrepreneurial.

I strongly believe that our steps to date have put TSA on the path to successfully meeting any challenge, no matter how unfamiliar or potent. But they are also fragile efforts, vulnerable to neglect and complacency. An entrepreneurial culture driven by an enterprise-wide dedication to constant reinvention is not the natural state for large organizations, let alone government agencies. Environmental factors and operational realities, such as budget uncertainties, geographic sprawl, and leadership churn tend to encourage an inertial hunkering down.

That persistent danger underscores the need to be conscientious in following through on the structural modifications TSA is undergoing. That is why it is of paramount importance to keep the momentum going. Like riding a bicycle, we need to keep moving and making headway or we risk falling over and reverting to the static organization, processes, and leadership mindset in which we were mired 18 months ago.

Over the next year to two years, the following initiatives are the priority efforts for solidifying gains and achieving the long-term envisioned state:

Implement the Human Capital Management Strategy

Institutionalize the TSA Training and Development Roadmap

Employ and evolve disciplined Acquisitions and Program Planning, Budgeting, and Execution (PPBE) processes

Inculcate innovation and an entrepreneurial mindset enterprise-wide through the Innovation Task Force

Configure operational and mission support governance structures to promote internal and external collaboration

Cultivate and advance partnerships with stakeholders across the transportation security ecosystem

During my confirmation process, I met with quite a few TSA employees. Many advised me to simply let them do the job they were hired to do – to protect the traveling public – and to have their backs when they do. They wanted to be what they joined to be: highly professional security officials protecting the traveling public and our nation's transportation system. I am immensely proud of the strides we have made together, and I am just as confident that TSA can become the next-generation counterterrorism organization it was called upon and aspires to be with the support and permission of our workforce, collaboration with our stakeholders, and a shared vision for delivering mission success now and into the future.

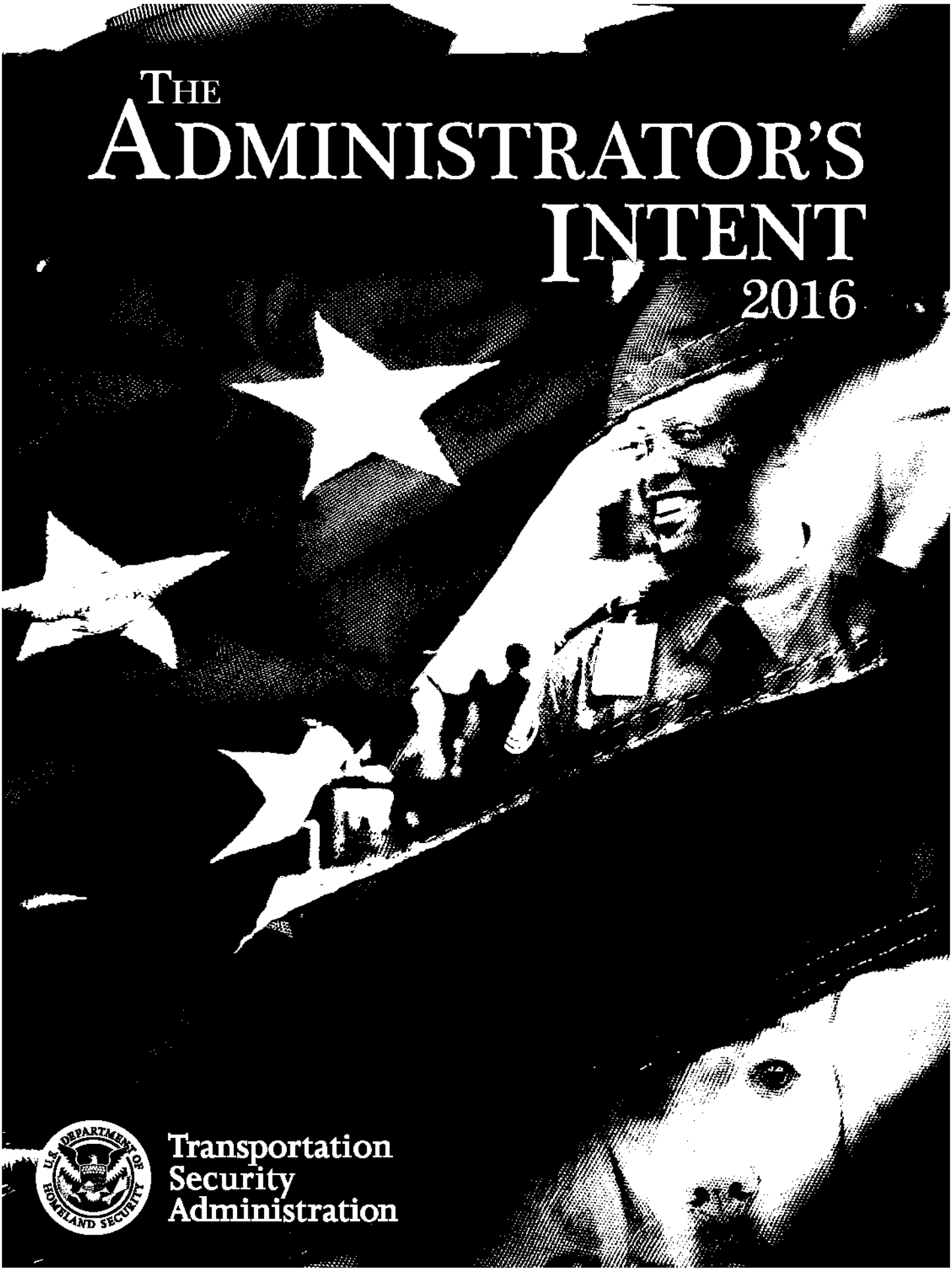
APPENDICES

I. The Administrator's Intent

II. Remarks as prepared for delivery at The Wilson Center by TSA Administrator Peter Neffenger, Washington, D.C.

III. Remarks as delivered at the Seton Hall University School of Diplomacy and International Relations by Administrator Peter Neffenger, South Orange, NJ

THE ADMINISTRATOR'S INTENT 2016



Transportation Security Administration

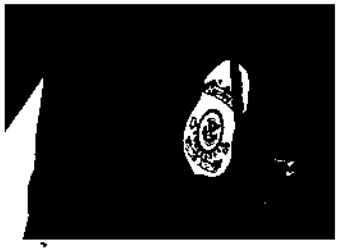
★ ★ ★

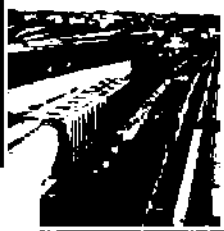
Table of Contents

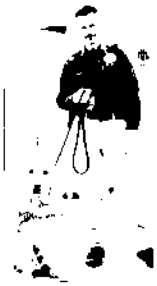
Letter from the Administrator	4
Focus on Mission	7
Invest in People	9
Commit to Excellence	11

About this Document

The Administrator's Intent will guide the Transportation Security Administration and is founded on our Core Values of Integrity, Innovation, and Team Spirit and guided by the principles of focusing on our mission, investing in our people and committing to excellence. Each principle reinforces the others and collectively, they will inform strategic, operational, and resource decision-making throughout TSA. This Intent lays out each principle to include its meaning, relevance, and applicability throughout the Agency and highlights the Administrator's priorities to focus our efforts in meeting anticipated challenges and risks.

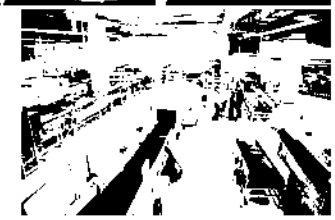






The Oath

I do solemnly swear that I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.



★ ★ ★

To the Women and Men of TSA:

Peter Neffenger
Administrator, TSA

It is my great honor and privilege to serve you and the American people as Administrator of the Transportation Security Administration.

We operate in a challenging, dynamic environment that requires our utmost dedication and professionalism. The United States faces a persistent threat from terrorist groups around the world and from homegrown violent extremists inspired by messages of hatred to do harm. Today, the threat is more decentralized, diffuse, and complex than ever before.

We swore an oath to defend our nation and secure our transportation systems and the people who use them. We must succeed in our important security mission. We will do this by adhering to our core values of Integrity, Innovation, and Team Spirit and following these three guiding principles:

Focus on Mission
We will put mission first and collaborate with our partners to succeed.

Invest in People
We will ensure our people are mission-ready, expertly trained, deliberately developed and led by value-based leaders.

Commit to Excellence
We will pursue mission excellence through a culture of constant improvement and adaptation to evolving threats.

I have full faith and confidence in you, and I thank you for your commitment to our mission and your support of one another.

★ ★ ★

Conduct ourselves in an honest, trustworthy manner at all times. Respect and care for others and the information we handle. Gain strength from the diversity in our cultures.

Have an enterprising spirit, striving for innovation and accepting the risk-taking that comes with it. Be courageous and willing to take on new challenges. Embrace and stand ready for change.

Be open, respectful, and dedicated to making others better. Have a passion for challenge, success, and being on a winning team. Build teams around our strengths.

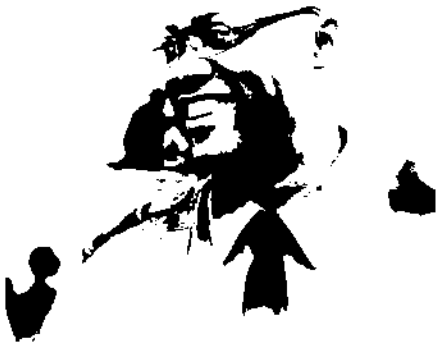
ISA

★ ★ ★

FOCUS ON MISSION

TSA will:

- ★ Leverage intelligence to inform operations and investments.
- ★ Employ a strategic, risk-based approach with measures of success to drive mission performance.
- ★ Sustain and expand security partnerships at home and abroad.



Our mission is second to none. We protect our nation, our fellow citizens, families and friends as they move about the Nation and the world. Ours is a critical national security mission. The attacks on 9/11 and the attempts that occurred since are a constant reminder of why TSA exists and why we come to work each day.

As a world leader in transportation security, we will continue to build and leverage the experience and skills of our people and the capabilities of our technologies to drive toward mission success. We will analyze and operationalize intelligence and apply risk-based principles to counter the plans of our determined adversaries.

We will employ a culture of operational evolution that constantly reevaluates assumptions, plans, and processes to achieve the highest level of mission excellence.

We are not in this alone. We will collaborate with federal, state, and local law enforcement agencies, private industry, and global stakeholders to strengthen our transportation systems and ensure the safety of our citizens when they travel.

From all walks of life,
we came forward to serve
at an agency built of innovation,
patriotism and steady virtue.

We are firm in our resolve
to not yield to terror.

★ ★ ★

INVEST IN PEOPLE

TSA will:

- ★ Invest in training to improve skills for all employees and build TSA's future leaders.
- ★ Expand the TSA Academy into a world-class transportation security and leadership training facility.
- ★ Emphasize the importance of standards, values and accountability.

TSA's strength, resiliency and ability to adapt are rooted in our people. Our professional and diverse workforce is dedicated to our mission and each other, puts service before self, and lives TSA's core values of Integrity, Innovation, and Team Spirit.

We must invest in the people who swore an oath to protect our Nation because their development and well-being is critical to the success of our mission. We will attract, develop, and sustain a professional, capable workforce and empower them to succeed and grow to their fullest potential. We will respect those we serve and those who serve with us by performing our duties professionally, courteously, and ethically.

We will increase our investments in training and education programs to strengthen TSA's professional foundation and build future leaders. A common foundation of training will connect our workforce to a unified culture, strengthen the focus on mission, and build esprit de corps.

Driven by a noble and critical mission
I proudly serve with integrity and professionalism
to protect my family, community and fellow citizens.

★ ★ ★

COMMIT TO EXCELLENCE

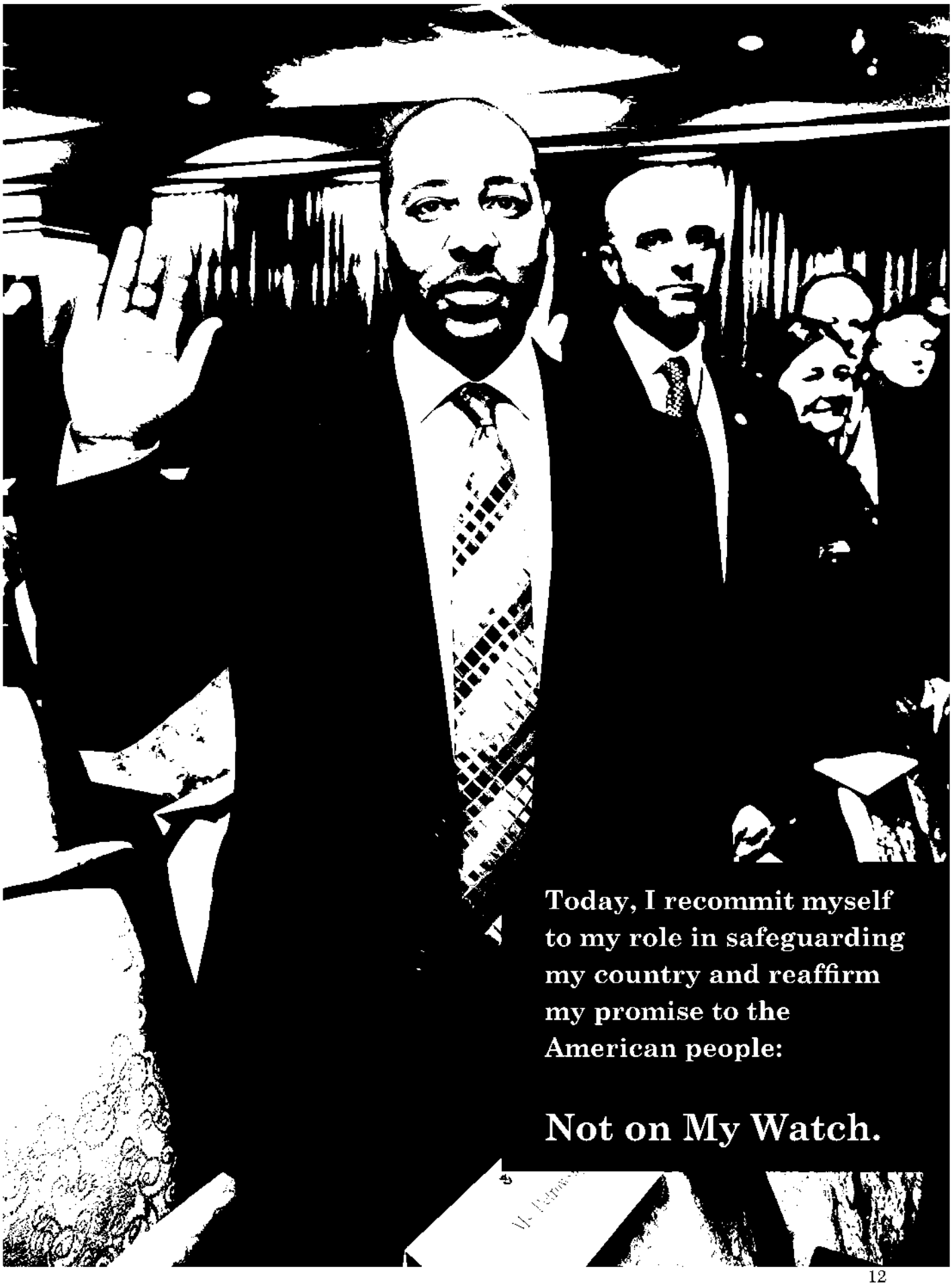
TSA will:

- ★ Adapt to evolving threats.
- ★ Set the global standard for transportation security.
- ★ Strengthen capabilities to develop, acquire, and deploy technology and other tools to drive mission success.

Our pursuit of excellence drives us to focus on the evolving threat. As our adversaries adapt, so will we. Given the dynamic threat environment, we will employ a strategic approach to ensure we strengthen our ability to detect, deter, and disrupt threat streams.

TSA will set the standard for transportation security in the fight against terrorism and will be the place where dedicated professionals want to work.

We will maximize the effectiveness of our people, processes and technologies while providing value through wise stewardship of resources and outstanding service to the traveling public. We will modernize our resource planning and deployment to obtain cutting-edge technologies to address evolving threats and enhance the capabilities of our people.


Today, I recommit myself
to my role in safeguarding
my country and reaffirm
my promise to the
American people:
Not on My Watch.

★ ★ ★

Forged on an anvil of cruel necessity
and blood shed innocently,
TSA was built urgently
in a time of war, to preserve peace.

From all walks of life, we came forward to serve
at an agency built of innovation,
patriotism and steady virtue.
We are firm in our resolve to not yield to terror.

Driven by a noble and critical mission
I proudly serve with integrity and
professionalism to protect my family,
community and fellow citizens.

Today, I recommit myself
to my role in safeguarding my country
and reaffirm my promise to the American
people:

Not on My Watch.

These words are inspired by the Cornerstone, a gift from The Department of Transportation commemorating TSA's creation and the transition in 2003 to the newly formed Department of Homeland Security.

APPENDIX II

Remarks as prepared for delivery at The Wilson Center by TSA Administrator Peter Neffenger, Washington, D.C.

Wednesday, July 13, 2016

Good afternoon and thank you for being here today. I would especially like to thank Jane Harman and the Wilson Center for the invitation to share with you some thoughts on TSA – what we have done this past year and where we are headed. I first met then Congresswoman Jane Harman in 2003 when I was working on the security of the Ports of Los Angeles and Long Beach. Jane is the best kind of friend – she listens to you, she thinks about what you have said, and then she challenges you to defend your ideas.

I also want to acknowledge Judge William Webster, former FBI Director and former CIA Director, and who currently chairs Secretary Jeh Johnson's Homeland Security Advisory Council. Thank you, Sir, for being here.

Every one of you has an image of TSA – a story about who and what we are. An idea of what we do, of how we do it, and perhaps, even, of whom we do it to. But I ask you to set aside your own stories for a bit and listen instead to the story we've been writing over the past year.

Introduction

In his book, "The Power of Habit," Charles Duhigg writes about when Paul O'Neill took over as CEO of Alcoa in 1987. O'Neill found a company in deep trouble. But in his first speech as CEO, he talked not about product lines, inventories, and falling profits, but about worker safety.

His words shocked the investment community. The word on Wall Street was to "sell!" One investor called his top clients and said, "The board put a crazy hippie in charge, and he's going to kill the company."

The rest of the story is well known. Focusing on worker safety had a ripple effect throughout Alcoa. It changed Alcoa's entire culture, and led to a reexamination of manufacturing practices and a cascade of innovations. One year after that speech, Alcoa's profits hit a record high.

Here's what Paul O'Neill said:

"I knew I had to transform Alcoa. But you can't order people to change. So I decided I was going to start by focusing on one thing. If I could start disrupting the habits around one thing, it would spread throughout the entire company."

Transforming TSA

When I came to TSA just over a year ago, I too found an organization in trouble and under intense scrutiny, and one that needed to change. We had to examine everything we were doing.

We had to look at our habits, and understand how they had informed our approach to our security mission – we needed to understand what determined success at deterring, detecting and disrupting those who would attack our transportation systems.

We needed to think differently. And we had to disrupt habits. But where do you begin?

During my confirmation process, I met with quite a few TSA employees, focusing particularly on those uniformed TSA officers who work on the front lines in our airports. I asked them what they thought about working for TSA. I asked them what it meant to be a Transportation Security Officer. I asked what they thought I should do if I got the job.

I got some interesting and enlightening answers. One officer said that she felt more part of the airport than TSA. A number of officers said that they felt their job had become one of getting people through security lines as fast as possible – and they were worried about whether things were getting past them.

Many advised me to simply let them do the job they were hired to do – to protect the traveling public – and to have their backs when they do. I found that they cared deeply about their work, their purpose and their identity. They wanted to be what they joined to be, highly professional security officials protecting the traveling public and our nation's transportation system, but they often felt like baggage screeners there to make the lines move fast. And as we began digging into the root causes of the Inspector General's findings, we kept returning to this fundamental notion of purpose and identity.

So, we began by collectively restating who and what we are – from top to bottom. We published our Intent. We said out loud that we were security professionals working in an intelligence-driven, adaptable counterterrorism agency focused on the security of our nation's transportation system. We retook the oath of office.

As it turns out, changing the way you define yourself, changes everything. The habits around one thing affected our entire agency. In Paul O'Neill's terms, the one thing we would focus on that would change everything was our identity. That single but important change set in motion the ongoing transformation of TSA. It led to changing the way we think about, prepare for, and execute our complex mission in what is perhaps the most dynamic and challenging threat environment we have seen.

Even as we have tackled the root causes of the Inspector General's findings and, thus far, successfully addressed the headline-grabbing wait times in the face of record air travel passenger volume, we have kept our focus on who we are and how we need to transform to meet future threats.

If we were to be security professionals, then we had to pay attention to delivering security.

The bulk of my professional career was spent in a mission-focused organization. I woke up every day thinking about the mission end of the organization – what do we have to do, why do we have to do it and how are we going to get it done?

With this in mind, our renewed commitment to our identity surfaced three very simple guiding principles. We would:

Focus on Mission

Invest in People

Commit to Excellence

To do that you need leadership, training, guidance, resources, and appropriate equipment.

Training is the foundation of mission success and a powerful tool in galvanizing and leading change. It provides consistency, develops a common culture, instills core values, improves morale, and it raises performance.

So we created a formal, professional training program. We began by retraining our entire workforce on mission essentials during August and September last year.

We followed that by establishing the first-ever full-time TSA Academy, at the Federal Law Enforcement Training Center in Glynco, Georgia, with the initial course offerings focused on training frontline Transportation Security Officers. This intensive, hands-on training focuses on consistency, culture, core values and performance.

We focused on our leaders through TSA's first executive leadership program, specifically tailored to the unique nature of the TSA mission. We changed the way we conduct our daily operations – asking our field leaders what they need rather than prescribing what to do.

In fact, we have overhauled our approach to operations, to include the establishment of a National Command Center to closely track daily screening operations and shift resources as needed to get ahead of problems before they arise; and for the first time we are doing this through daily, direct, airport-by-airport collaboration with airlines, airports, the travel industry and other transportation system professionals.

TSA is an integral element of an effective and efficient system. That's an incredibly important point. We cannot act in isolation. To succeed we really need to be fully integrated with our many partners – airlines, airports, industry, other federal agencies, state and local governments and, of course, Congress. This past year Congress was there for TSA as a real partner in understanding our needs and helping us get the resources we need:

We have fully integrated intelligence and analysis into our operational planning.

We are reforming acquisitions and human resource management.

In partnership with airlines and airports we have begun making improvements to checkpoints.

We have entered into public-private partnerships with a number of airlines to purchase and install new automated screening lanes to greatly improve checkpoint throughput, increase effectiveness and improve the passenger experience.

And it is real improvement – you'll see these new, automated lanes in many airports before the end of the year. These efforts are paying real dividends – in effectiveness, in efficiency and even in employee morale. So, focusing on identity really did change everything.

Who We Are

And that's important, because TSA is truly the retail face of government. Who we are matters to over 2 million travelers with whom we interact each day. And it is an intimate and often stressful interaction – for both traveler and TSA officer. We examine your things. We examine you. And sometimes we touch you physically.

We do that because there are very real, persistent and evolving threats to transportation. Terrorist groups and individuals remain intently focused on doing us harm and they are creative, determined and adaptive.

Vision

So what comes next? That's the question I am most interested in answering. And it is a question that TSA cannot answer by itself.

Solving immediate, pressing issues about effectiveness and long lines has been critically important. Putting automated lanes into airports is a must do – and will make all our lives significantly less stressful as we travel over the next year.

But we can't stop there. These measures alone do not transform the system. They do, however, give us the breathing room to move to an entirely new way of thinking about security.

Much has changed over the years – we have better, more fully integrated intelligence, our technology is more capable, our workforce is more professional and we understand risk better.

But in the aviation environment in particular, we still talk of airport perimeters, public areas, checkpoints, sterile areas. Most of the physical security takes place at the checkpoint, and the checkpoint by definition aggregates a lot of security elements in a fairly confined space. Remember, checkpoints were inserted into what used to be open airports.

But what if we were to re-envision the entire system as an integrated whole? From reservation to destination. More fully integrating information and activity among all the elements and players in the system – disaggregating and distributing security throughout the system – reducing friction to the traveler while at the same time increasing security effectiveness.

We need to think and design less in terms of checkpoints and barriers and more in terms of a security environment in which there are many security partners.

We may never return to the levels of openness we enjoyed prior to the tragedy of 9/11. But, we can envision a future in which security is more seamless – more transparent even – eliminating some of the things that create friction for us all.

Recent world events – the detonation of explosives on aircraft above the Sinai and Mogadishu, the airport and metro bombings in Brussels and the recent attack at Istanbul airport illustrate the imperative to rethink the security environment.

Perimeter barriers and checkpoints serve a purpose, but they have to be integrated into a much larger security environment.

TSA's new Innovation Task Force is working on this. This task force is focused on what comes next. They are taking a fresh look at the entire system. They are working with public and private partners to provide a platform for government, industry and stakeholders to gather requirements for approaches to disrupt current practices and accelerate the development and deployment of new technologies and concepts of operation.

However, the real value of this task force is not only the security enhancements it will enable, but its unconventional approach is an example of how we are changing the way we think. That's key for one simple reason, those who would harm us are as creative and resourceful as they are ruthless.

We've taken some important steps: the expansion of trusted traveler programs, the advances in automated lanes I mentioned and new and enhanced screening technologies. And, these pave the way for better biometric security such as iris and fingerprint scanners, and even facial recognition.

Such advances, for example, could lead to the complete elimination of boarding passes and document checks for those

willing to opt into the system. This begins to create the potential for a very different security environment.

Indeed, we will need to answer important questions about privacy and civil liberties. But we need not sacrifice our rights in order to develop and implement effective security.

Like the many great agencies with whom we work, TSA must continuously evolve, adapt, invent and reaffirm its security mission. So in coming to a full understanding of TSA's identity, we can better appreciate its need to evolve and transform.

TSA has been charged with an enormous responsibility to protect our nation's transportation systems, but we've learned that it is a shared responsibility and that the more we share responsibility the better the results.

Congress, airlines, airports, industry, federal, state and local governments, law enforcement – everyone has an important role to play.

So, to our partners and stakeholders in and out of government, I ask that you engage with TSA – aggressively – to challenge conventional thinking about the security environment to address the ever-changing and evolving threat.

So, that's who we are. That's what we're striving for. That's what some 60,000 TSA professionals have taken an oath to do.

Thanks again for being here today, I look forward to our discussion.

###

APPENDIX III

Remarks as delivered at the Seton Hall University School of Diplomacy and International Relations by Administrator Peter Neffenger, South Orange, NJ

Tuesday, November 29, 2016

Thank you Mo, and thank you to Seton Hall for inviting me here today; Dean Andrea Bartoli; Father Brian Mozas; our Master of Ceremonies Francesca Regalado; Associate Dean Elizabeth Halpin and Assistant Vice President Daniel Nugent.

I also want to recognize Dennis Egan – from Rutgers University; Dr. Peter Forster – from Penn State University; and, of course, a hearty welcome to all the folks from TSA who joined us here today.

I like telling the story of TSA. And I hope that as you listen, you'll set aside your own notions of who and what we are, and maybe come to understand and share my excitement.

Earlier this year in speaking to the challenges I found at TSA, I talked about identity - about who, and what, we are. I said that our transformation began by changing the way we define ourselves. We said out loud and collectively that we were security professionals, working in an intelligence-driven, agile, adaptable counterterrorism agency focused on the security of our nation's transportation systems. We all retook the oath of office. We learned that changing how we defined ourselves changed everything.

Today I'd like to continue that story – by telling the next chapter and highlighting how that renewed sense of identity allowed us to become more innovative and entrepreneurial.

A Shipping Story

But I'm going to start with another story – one from my maritime background.

Malcolm McLean was one of seven children of a North Carolina farm family growing up during the Great Depression. Starting with a used truck he bought to help his family get goods to market, he eventually built the fifth-largest trucking company in the United States. So, that's interesting, but not the story I find illustrative.

Here's the one I like: One day Malcolm McLean was sitting in one of his trucks on the docks in Hoboken, New Jersey,

waiting, and waiting, to transfer his truck's contents to a ship, and watching as the longshoremen loaded cargo net after cargo net moving a few boxes at a time to the ship's hold. It was driving him nuts – he thought it would be a lot easier to just pick up his truck trailer and load it straight onboard. That simple, disruptive thought stuck with Malcolm McLean for 20 years and, in 1956, he made his idea a reality and, standing near those same docks, watched as the very first container ship – his ship – filled with shipping containers set out to sea. That voyage spurred the complete transformation of the shipping industry.

There are a number of useful lessons from this story, but here's the one I like – and how I choose to view what Malcolm McLean did. He wasn't just looking at an inefficient process for loading ships – it was certainly that – I think what McLean saw was that the way in which ships were loaded was a crippling component of an otherwise efficient system of transporting goods from origin to destination – a system that had become dramatically more efficient through improved highway infrastructure, warehousing, larger and more reliable conveyances, and the like.

To most people the system worked well enough, because most people only think about their individual piece of the system. Longshoremen were doing what longshoremen always do.

Now I didn't know Malcolm McLean, but I think he instinctively understood that the real mission – the "job" – was to move "stuff" from origin to destination safely, efficiently and effectively. Trucking companies like his were part of a vast and interconnected system. He transformed the system, because he understood the system.

Transforming TSA

Like Malcolm McLean, TSA had to understand that we, too, were part of a vast and interconnected system, and that our actions directly affected the security, efficiency and effectiveness of the entire transportation system. We had to understand our real mission; our true purpose; and why we exist.

When I got to TSA in July 2015, I found an agency in crisis and under intense scrutiny. There had been testing failures, allegations of questionable management practices and it was disconnected from the industries and public it served. Indeed, TSA's public image was largely that of long security lines punctuated by a uniformed security officer at an airport checkpoint. TSA, for many, was the agency that got in your way and intruded upon your travel.

We are the retail face of government, and you have to pass by us if you want to travel on an aircraft. We examine your things, we examine you and sometimes we even touch you physically.

I found an agency that to a large extent had adopted this image and one that had become inured to criticism – in fact, one individual said to me during an early briefing, "Boss, you have to understand that people don't like us – it just comes with the job". We were hunkered down, disconnected and resistant to change. We had become the things we do.

But I also found dedicated people, some with many years of service to TSA – some had even been at the agency since "rollout", the wonderfully evocative term used with justifiable pride to describe the herculean and quite remarkable effort to stand up a nearly 60,000 member organization in mere months.

Think about the task they faced 15 years ago:

Replace a disparate, disconnected system of private screening contractors at nearly 450 airports across the country with a federal workforce, without interruption of operations.

Establish security oversight for every mode of transportation – aviation, rail, transit, over the road buses, maritime, and even pipelines. If it moves, protect it.

Picture people in borrowed offices working long hours sketching on note pads the thousands of things needed to create an operating agency out of whole cloth.

Do all of this in the anxious, uncertain months following 9/11, when it seemed as if the next attack would happen at any moment. And in fact almost did in December 2001, when an individual attempted to detonate the explosives packed into the soles of his shoes on a flight from Paris to Miami.

This job was serious business. The system had failed, and they had to fix it, and fast. Under intense pressure, they had to be innovative and daring. And people from all walks of life – the private sector – airlines, airports – the military, the FAA, indeed from all across government – all came together to do something that had never been done before.

We needed to recapture that spirit of innovation and daring. We needed to reconnect to the sense of purpose and mission that had energized TSA's "rollout". That's easier said than done – there's a lot of resistance to doing things differently. Traditionally, government nurtures the status quo, whereas, entrepreneurial thinking points in a new direction and thrives on change.

But, as the Malcolm McLean story illustrates, we needed to get past entrenched thinking in order to see ourselves as part of a larger system – in our case one that ensures the security of our Nation.

To do so, we needed to overcome the tendency for large organizations to get locked into a set way of doing things.

Think about an operating agency, which is what we are. We have to do something every day – just like the longshoremen working on the docks. There's little incentive to change because the status quo works well enough and we have an entire internal system built to support it. We've invested a lot in the system. It's comfortable and predictable – and changing it would be hard and disruptive.

TSA screens some 2 million travelers every single day, and we have a lot of process built around that. But TSA is much more than passenger screening – that's simply one of many activities that we do.

What we really do is secure a vast, complex interconnected global transportation system that underpins our economic health and in the United States employs one out of every seven workers.

And we don't, and can't, do this alone. We don't own the system. Airlines, airports, rail operators, transit providers, trucking and shipping companies, pipeline operators, other government agencies, travelers and many more are key players and co-owners in the security of the system. It turns out that our mission includes aligning all of those elements to work together with us to keep the transportation system operating efficiently and securely.

Training

So, where did we begin?

First, we had to figure out how to begin to drive change. It starts by finding the change leaders in your organization and giving them permission, encouragement and support. Here's an example:

TSA had no centralized, coordinated or consistent approach to training. But training is the foundation of mission success and a powerful tool in galvanizing and leading change.

It provides consistency, develops a common culture, instills core values, improves morale, and it increases performance – something we needed to do in the wake of legitimate concerns about TSA.

So, I asked a lot of questions about training. As it turned out TSA had a creative training and development team that had a solid plan to build a full-time, resident TSA academy that would provide consistent, disciplined and professional training across the workforce. But, budget cuts, internal bureaucracy and organizational inertia had stymied the plan

and we were years, if ever, from seeing its realization.

But, I liked the idea of an academy – it was innovative and forward-thinking, and it addressed many of the challenges we were facing. I asked if we could accelerate and put it in place in three months. In other words, I asked my team, "If I give you permission and support, could you do it now?"

No joke; they came back later that day and said, "Yes". Of course, we still needed money, a place to build it and approval from the Administration and Congress – but assuming we could get that, we could have our academy.

So we went to work, we built our case, got support from the President and Congress and three months later – last January to be exact – we established the first-ever full-time TSA Academy at the Federal Law Enforcement Training Centers in Glynco, Georgia.

The key point here: We found talented and creative people within and then gave them permission and support to be entrepreneurial, to take risks, and then, from the top of the organization, aggressively drove the change.

And, interestingly, as we transformed training, we reconnected to our mission and that, in turn accelerated our thinking about how we could drive change across our agency.

We've used this approach over the past year and a half to stimulate innovation and reconnect with the entrepreneurial spirit of rollout. But, changing processes and systems wasn't enough. We also needed a way to continue to grow and sustain the effort.

Here's how we're moving down that road.

The Innovation Task Force

At the busiest airports, we needed a faster means of moving people through the checkpoints given the year-over-year dramatic increases in the number of travelers moving through airports. You all remember the long lines in airport security. These long lines were more than just an inconvenience and frustration – they were a real security concern.

Large crowds in public places are attractive targets for terrorists. I know, I had just arrived at Brussels airport when suicide bombers killed 32 people and injured over 300 more. I witnessed the aftermath. So, moving people more efficiently into secure areas was more than a convenience to travelers, it was a security imperative.

We had an intriguing opportunity – automated screening lanes that were already in operation in London and Amsterdam. These seemed like a pretty good idea. They could move people faster through the checkpoint at the same or better level of security effectiveness – although in a year over year cycle of tight budgets, a daunting number of airports in which to invest, and a slow and cumbersome federal acquisition process, introducing these would not be easy.

There was also a fair amount of resistance – we'd need new procedures and training. But I was determined to find a way to do this.

It was clear that our interest aligned perfectly with the airlines. We had already begun to change our relationship with them from adversarial to collaborative. We were partners in security, and that opened new opportunities. They needed us to be more efficient and effective in moving their customers through the checkpoint and we needed to do so for the reason I just mentioned, but without compromising security.

So I wondered, what if we could work with the airlines to buy a couple of these automated lanes – just as a pilot project?

I floated the idea, and Delta was the first to take a chance and fund our experiment. They bought two lanes, installed them in Atlanta and gifted them to the federal government – a true public-private partnership. We established an Innovation Task Force to manage the project.

Now here's the amazing part: We went from idea in March to implementation in May – just nine weeks – not years – and these lanes do, indeed, move people more efficiently. Our officers love them, and travelers like them. Today several major airlines are pitching in with millions of dollars – United, American, Delta – and we're installing automated lanes in major airports around the country. You can see them right now not far from here at United's Terminal C at Newark Airport.

Turns out this pilot project became a catalyst for innovation throughout TSA. It also taught us that we needed an incubator for innovative and entrepreneurial ideas. Remember, an operating agency is focused on its everyday activities and processes, you can't mess that up, so we needed a place in which to surface, examine and nurture change, and then introduce it into operations. So we formalized the Innovation Task Force as a permanent entity – we assigned creative, thoughtful and energetic people from within TSA. We partnered with the private sector.

We also wanted the Task Force to be a receptacle for new and creative ideas from the outside. The Task Force's job is to reimagine the system and become a driver for innovative, entrepreneurial thought – to ask the questions, "How can we evolve the transportation security system to meet the threats and challenges of tomorrow?" And, "How can we weave security into the very fabric of the system in the same way that safety has been integrated into every aspect of transportation?"

The Threat Environment

So why is all of this important – all of this talk of innovation and entrepreneurship? Because today's threat environment is more dynamic and challenging than ever before. There are very real, persistent and continuously evolving threats to transportation – this past year alone we saw the detonation of explosives on aircraft above the Sinai and Mogadishu, the airport and metro bombings in Brussels, the attack at Istanbul airport, and the tragic attacks in Paris, Nice, San Bernardino, and Orlando. Terrorist groups and individuals remain intently focused on doing us harm and they are creative, determined, adaptive and ruthless.

Lessons Learned

So, what are the lessons here?

First, know your mission: The core mission that everyone needs to be connected with. Like the janitor at NASA who said when asked what he did – "I help to put a man on the moon." That's connection to the mission!

Second, no one person is the change. You need to look within the organization and identify those talented, creative and experienced folks that are ready to embrace a new way of thinking. Many will not be receptive, but there will be a core group of daring, risk takers ready to take the plunge and follow you. Then give them the permission and the cover they need and you'll be stunned by the results.

I had a mentor years ago who once said to me, "Don't stand and point to where you want to go, just go there! People will follow."

Third, in evaluating an organization's shortcomings and failures, there is a strong temptation to blame people – don't. It's generally the system that fails. Put your faith in the people, and they will help you fix the system – in fact they will show you the many pathways. In my experience, very few people, if any, wake up in the morning and say, "Gee, I wonder how I can screw up my job today?"

Fourth, find some quick wins in order to show the rest of the organization what's possible. Our innovation task force, our training academy and working with the airlines to install automated lanes are significant actions. Those early wins showed the organization that we can change, and that change can be good.

Fifth, if you find yourself in crisis, resist the instinct to just survive, get through it and move on. You need to run to the crisis and embrace it! A crisis surfaces important information about an organization that allows you to address and implement long-term solutions. A crisis may be traumatic, but it often is a necessary shock to the system and can lead to meaningful, effective change.

Finally, you have to be daring. Being afraid to take risks is actually the riskiest position because it fosters a static approach that exposes vulnerabilities no matter what you do for a living. Malcolm McLean put the industry that made him millions at risk, but in doing so, he transformed that industry.

Conclusion

So today, I see TSA differently from when I arrived.

It's interesting. As I was going through confirmation, there were a number of people who warned me that TSA was an agency in trouble with low morale. They said it had an impossible mission, and that it was in many respects, unmanageable. Some even said it couldn't be fixed. I just didn't believe that. As I said earlier, people don't fail, systems do – and systems can always be fixed.

TSA has been charged with an enormous responsibility to protect our nation's transportation systems – what we do matters.

To be sure, we are not yet where we need to be, but we know where we're going. We are a good and proud agency, and we have changed dramatically over the past year and a half. We've done that by aggressively examining and questioning ourselves, by reaffirming our identity, by understanding our true mission, by reconnecting and collaborating with the industries and the public we serve and by becoming innovative and entrepreneurial.

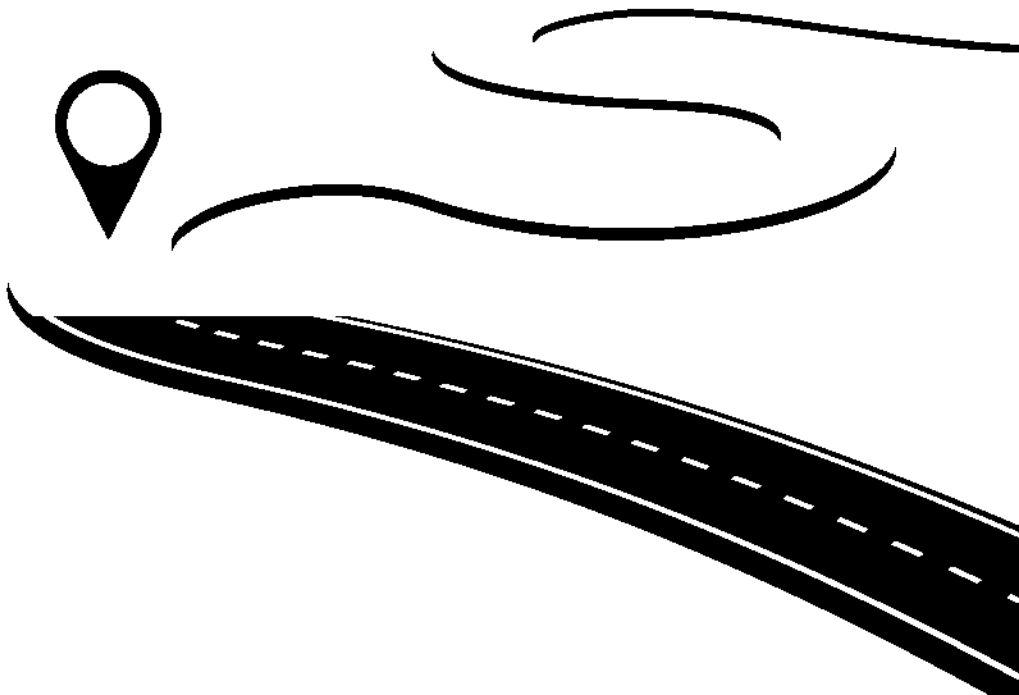
So here's what I'll leave you with: Know your mission – the real mission. And then, no matter what your role is, know that you, too, can drive change. You, too, can be creative, entrepreneurial, and innovative – you just have to be daring. You just have to take that first step.

And give people permission and support.

And, please say thank you to the Transportation Security Officers who keep you secure.

Thanks again for inviting me here, I look forward to our discussion.

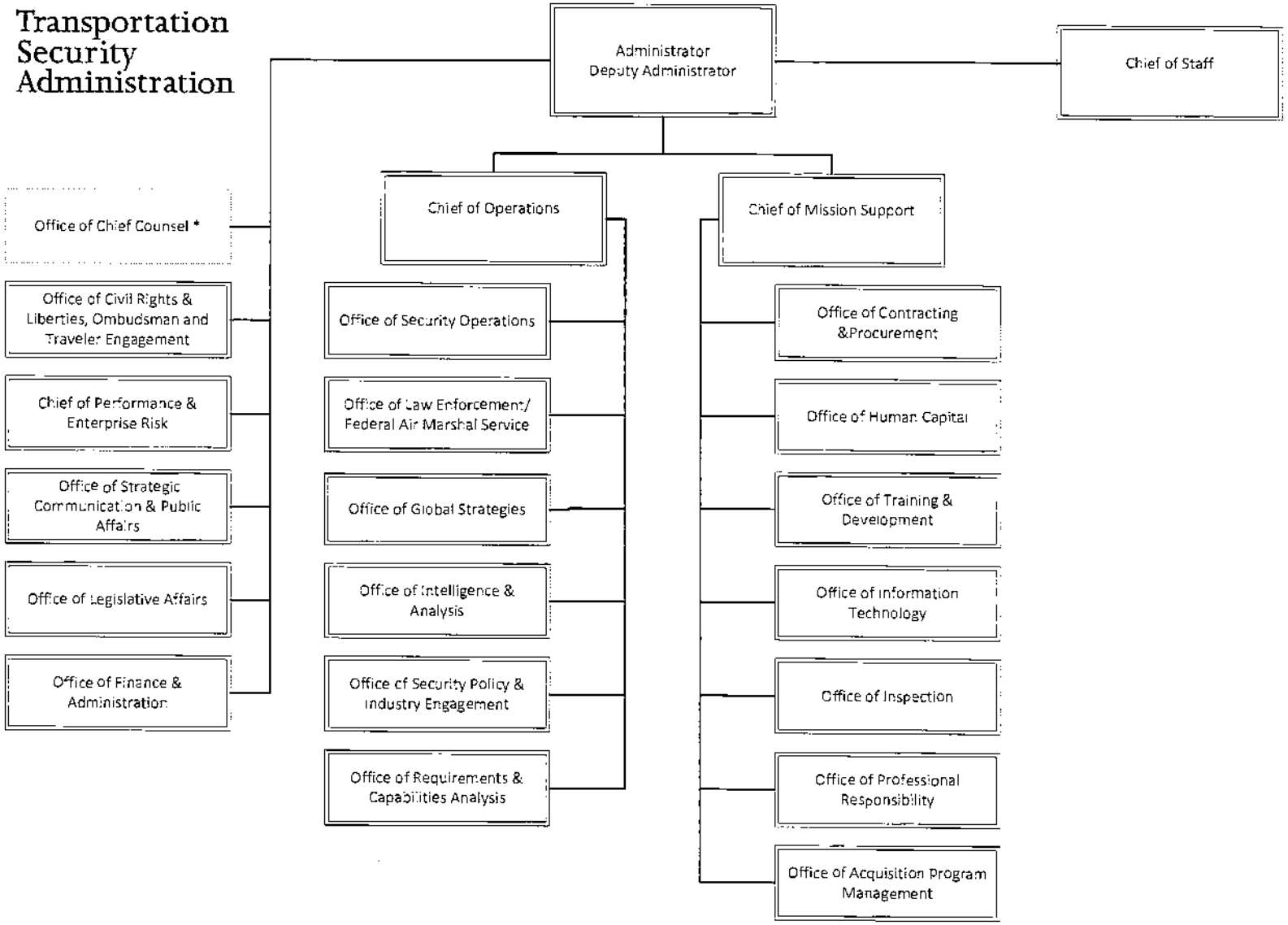
###



Transportation Security
Administration

For information, contact TSA Public Affairs: tsamedia@tsa.dhs.gov or 571-227-2829

Transportation Security Administration



*The Office of the Chief Counsel reports to the Department of Homeland Security, Office of the General Counsel

Approved by: Huban A. Gowadia
Deputy Administrator

Signature:

Date: 17 Oct 16

DHS Transition Issue Paper
Screening and Vetting

OVERVIEW

- Every day, DHS vets millions of individuals traveling to, from, or within the United States; applying for citizenship and immigration benefits; or seeking credentials, benefits, or access to secure areas of the nation's transportation or critical infrastructure.
- DHS, in partnership with our law enforcement and Intelligence Community colleagues, leverages a range of information and processes to conduct vetting and screening that support the prevention of terrorism and other operational missions.
- DHS utilizes biometric and biographic information collection; in-person interviews; research and analysis; database vetting and bulk data sharing; and publicly-available information to make risk determinations and inform decisions.

Current Trends/Operational Drivers

- **Shared/Enterprise Services:** DHS is increasingly sharing vetting services across components, where appropriate, and utilizing enterprise services. For example, the Transportation Security Administration (TSA) conducts vetting for the chemical facilities access security program run by the National Protection and Programs Directorate (NPPD). DHS also maintains and operates a biometric database (IDENT) that is used broadly by the interagency.
- **Pushing Security beyond the Borders:** To support DHS's efforts to identify and address international threats as early as possible, operational programs (such as CBP's Preclearance and Trusted Traveler Program) provide opportunities for vetting travelers abroad and prior to travel to the United States, allowing for more efficient allocation of resources and increased ability to focus on unknown or potential threats.[1]
- **Social Media:** DHS is working to expand its current uses of social media to enhance existing vetting processes. Criminals and terrorists, whether intentionally or not, have provided previously unavailable information via social media that identified their true intentions.
  - Social media is currently used by DHS Components for different operational or investigative purposes. DHS established a Social Media Task Force in December 2015 to examine current and potential uses of social media and how DHS could best expand its use (for screening and vetting programs).
  - In 2016, DHS conducted a number of pilots to automate bulk vetting (with manual review) of social media information across a number of high priority application populations, including refugees and Visa Waiver Program travelers.

[1]CBP's Preclearance program, operating at 15 locations worldwide, allows for advance inspection of passengers before they board U.S.-bound flights. Additionally, CBP's range of international Trusted Traveler programs, such as Global Entry, provides pre-vetted and approved, low-risk travelers expedited clearance upon their arrival in the United States.

~~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.~~

DETAILED DISCUSSION

An April 2015 DHS study estimated that for all its traveler and screening vetting programs DHS spends approximately $7 billion per year utilizing more than 60,000 employees.[2]

- U.S. Customs and Border Protection (CBP): CBP is tasked with securing the Nation's borders. CBP has adopted a comprehensive strategy to border management and security, combining customs, immigration, and agriculture inspection functions. On an average day, CBP processes, through a combination of vetting and inspections, over 1 million citizens, immigrants, and non-immigrant visitors through the U.S. border. CBP uses its vetting capabilities to screen Trusted Travelers for expedited processing, allowing a more efficient allocation of officer resources for the identification of unknown or higher risk travelers.
- U.S. Immigration and Customs Enforcement (ICE): ICE works with state and local law enforcement officials to (a) prioritize the identification, location, and arrest of at-large criminal aliens who pose a serious threat to national security and community safety; and (b) to identify and remove criminal aliens in local, state and federal penal institutions and/or those who are at large in our communities. In addition, to further the integrity of the U.S. immigration system, ICE has developed, in coordination with CBP and the Department of State, a pre-visa-issuance screening program to identify subjects who are ineligible to receive visas for travel to the United States.
- DHS Office of Biometric Identity Management (OBIM): OBIM, a subcomponent of the National Protection and Programs Directorate (NPPD), is the lead entity within DHS for storing, matching and analyzing biometric data, and associated biographic and encounter data. OBIM operates the Automated Biometric Identification System (IDENT), which contains both derogatory and non-derogatory information received from components and other Federal partners. DHS uses this biometric database to assist vetting persons seeking admission to the United States, a visa, an immigration benefit, or a transportation credential or benefit. It is also available to interagency partners, such as the Department of State, FBI, DOD and others.
- Transportation Security Administration (TSA): TSA screens individuals to prevent them from unlawfully carrying a weapon, explosive, or incendiary either into the sterile area of the airport or onboard a commercial flight. TSA also vets individuals flying to, from, over and within the United States, and individuals seeking regular access to the transportation infrastructure against the Terrorist Screening Database. TSA's risk-based, intelligence driven screening is designed to promote both national security and lawful travel. This approach allows TSA to allocate screening resources expeditiously.
- U.S. Citizenship and Immigration Services (USCIS): USCIS is charged with the adjudication of immigration (and limited non-immigration) benefits. USCIS's mission includes granting the appropriate immigration benefit to those who qualify and denying benefits to those who are not qualified. USCIS has longstanding partnerships with screening agencies within the intelligence and law enforcement communities. USCIS is responsible for the annual adjudication of over 8 million applications for benefits.
- U.S. Coast Guard (USCG): USCG collects, integrates, and analyzes information concerning vessels operating on or bound for waters subject to the jurisdiction of the U.S., including

[2] Enterprise Wide Application of Risk Based Security

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.

information related to crew, passengers, cargo, and intermodal shipments to ensure safety and security of the U.S. maritime domain.

- The Screening Coordination Office (SCO): SCO located with the Office of Policy, has responsibility to coordinate across DHS Components and with interagency partners on the development or revision of Department-wide policies related to the screening and vetting of people, and USG-wide screening and vetting polices with a DHS nexus.

Issue Background

- Screening of International Travelers: The screening and vetting of immigrant and non-immigrant travelers to the United States is a multi-layered interagency process.
  - DHS plays a leading role in the protection of the U.S. border and integrity of the immigration system, to include review of applications for certain immigration (and limited non-immigration) benefits such as permanent residence and naturalization.
  - The Department of State (DOS) has responsibility for the adjudication of all visa applications (immigrant and non-immigrant).[3]
  - Other federal screening partners, to include the intelligence and law enforcement communities, work in concert with DHS and DOS to identify travelers who may represent a threat to national security.
- Refugee Screening: The screening of refugees has been a major effort for DHS and its partners in FY2016 as the U.S. Government increased its admissions goals in response to the crisis in Syria.
  - The U.S. Government has succeeded in meeting these humanitarian goals while maintaining a rigorous screening process that protects national security; refugees are now subject to the most demanding screening and vetting of any applicant for immigration, or other travel benefits, to the United States. An estimated 85,000 refugees, to include over 10,000 Syrian refugees, were accepted into the country during FY2016.

Courses of Action: Screening and Vetting Recommendations

- Increase Pro-active and Recurrent Screening: DHS components are pursuing various means to conduct pro-active and recurrent screening for various populations, such as:
  - Certain non-U.S. citizens to whom benefits were granted in the past, but who do not currently have applications pending, such as permanent residents who have not filed naturalization applications.
  - TSA-vetted populations, to include credential holders and applicants, who receive recurrent vetting for potential terrorist connections but not for criminal violations.
- Expand Capacity to Vet against Social Media: Social media is a prominent component of modern society, and DHS's efforts to protect the homeland must progress and adapt as society evolves. DHS must continue to invest in developing the technology and processes needed to make effective use of social media information while protecting privacy, civil rights, and civil liberties.
- Increase Intra-Departmental Information Sharing: To increase the effectiveness of individual component mission operations, DHS can benefit from increasing automated processes in which information on specific individuals is shared for the broadest operational use possible.

[3] DHS participates in the vetting of visas, as well is the lead agency with responsibility for visa policy.

~~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 (Vetting and Screening)

- Federal Government: Central Intelligence Agency; Department of Defense; Department of State; Federal Bureau of Investigation; National Counterterrorism Center; National Security Agency; and the Terrorist Screening Center
- State and Local Law Enforcement Agencies
- International Partners
- Private Sector

Additionally, all screening and vetting programs within DHS work closely with the DHS Office of Policy, Office of Privacy and DHS Office for Civil Rights and Civil Liberties. All DHS vetting programs build information security, privacy, and civil rights and civil liberties policies and practices into their operations.

~~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
Trade Security, Facilitation, and Enforcement

I. Overview

With the creation of the U.S. Department of Homeland Security (DHS) by the Homeland Security Act of 2002, U.S. Customs and Border Protection (CBP) assumed responsibility for enabling legitimate trade and enforcing trade laws at the United States border, including its Ports of Entry (POEs). Additionally, U.S. Immigration and Customs Enforcement (ICE) assumed responsibility for the investigation of U.S. importers, companies, and other entities that attempt to circumvent lawful trade mechanisms, including payment of required duties. Finally, the U.S. Coast Guard (USCG) assumed responsibility for ensuring a secure international supply chain by performing security assessments of anti-terrorism measures at the ports of approximately 150 countries that conduct maritime trade with the United States.

CBP is the primary U.S. Government component charged with monitoring, facilitating, and regulating the flow of goods imported through coordinated border management at our 328 POEs. Key challenges that CBP faces with the 21st century global supply chain include the exponential increase in use of e-commerce, the next generation of just-in-time delivery capabilities, and the ever-increasing complexity of the international trade environment. As the volume of international trade increases and technology advances, CBP must accommodate this growth while continuing to facilitate safe and legitimate trade in a timely manner. CBP meets these challenges through the following three distinct but interrelated efforts: *Trade Security*, *Trade Facilitation*, and *Trade Enforcement*.

ICE is the largest investigative component within DHS, with an extensive portfolio of enforcement authorities, including those related to commercial fraud. ICE aggressively pursues crimes and investigations related to dumping and countervailing duty evasion schemes, pharmaceutical smuggling, tobacco smuggling, and other border related trade crimes. Additionally, ICE investigates intellectual property violations involving the illegal importation and exportation of counterfeit merchandise and pirated works, as well as associated money laundering violations.

Recognizing the need to work with other law enforcement, as well as stakeholders, ICE leads various coordination efforts, such as the National Intellectual Property Rights Coordination Center (IPR Center), which brings together 23 partners in a task force setting. CBP holds a Deputy Assistant Director position at the IPR Center, and together, the two components work to enhance economic competitiveness, protect American consumers and the U.S. economy, and enforce laws and regulations against trade fraud in an increasingly complex international trade environment.

~~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.~~

Customs laws and recent legislative developments, namely the enactment of the **Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA)**, enhance DHS' authorities and impact the balance of trade security, facilitation, and enforcement. TFTEA, enacted on February 24, 2016, is the first comprehensive authorization of CBP since DHS was created in 2003. TFTEA strengthens CBP's ability to protect Intellectual Property Rights and Antidumping and Countervailing Duty laws through improved enforcement capabilities, prohibits the import of products made by forced labor, and supports CBP's facilitation and enforcement initiatives such as the establishment of the Centers of Excellence and Expertise and the implementation of the Automated Commercial Environment (ACE). TFTEA supports DHS' efforts to *protect U.S. economic security* through trade enforcement; *collaborate with the private sector* through direct industry engagement; and *streamline and modernize processes* through business transformation initiatives to meet the demands and complexities of a rapidly evolving global supply chain.

II. Detailed Discussion

Where do DHS missions align with or impact this issue? DHS Mission Two (2), as defined in the *DHS FY 2014-2018 Strategic Plan*, outlines the following three goals, which directly align with the issue of this paper, *Security, Facilitation, and Enforcement of Trade*.

DHS Mission 2 Goals	CBP, ICE, and USCG Action
Goal 1: Secure U.S. air, land, and sea borders and approaches.	**Trade Security**: • CBP protects the American consumer from illegal goods to safeguard the nation from threats to economic security and public safety. • ICE contributes to the security of the air, land, and sea borders by conducting criminal investigations that prevent fraudulent trade practices and the importation of counterfeit goods. • USCG enhances the security of the international supply chain through its foreign port assessments and through identification of potential offshore risk and implementation of security measures to reduce those risks.
Goal 2: Safeguard and expedite lawful trade and travel.	**Trade Facilitation**: • CBP facilitates the smooth flow of safe and legitimate trade in a complex global trade environment. • ICE safeguards lawful trade by working with law enforcement partners and industry to stop activities that undermine legitimate trade.
Goal 3: Disrupt and dismantle transnational criminal organizations and other illicit actors.	**Trade Enforcement**: • CBP enforces and sanctions bad trade actors and safeguards the safety of the American people. • ICE, through its criminal investigations, disrupts and dismantles transnational criminal organizations and illicit actors.

1. Trade Security – Protecting the American People and Borders from Illegal Import and Entry of Goods

Each year, approximately 25 million cargo containers arrive at U.S. POEs. DHS works closely with the trade community through its security efforts to ensure that the contents of each container do not pose risk to the health and safety of the American people and economy.

All cargo that enters into the United States from any foreign territory may be subject to physical examination by the U.S. Government to verify its admissibility. DHS protects the United States against terrorists, weapons of mass destruction, and products that may harm the American consumer. For example, DHS uses an intelligence assessment to determine if a foreign country has effective anti-terrorism measures at their ports, and in cases where DHS determines that the international security standard is not met, the USCG makes a public notification through a Port Security Advisory and a Federal Register Notice and imposes Conditions of Entry on vessels arriving from those ports, requiring those vessels to take additional security measures to prevent them from bringing potential terrorists or weapons of mass destruction into the United States. All cargo flown on passenger aircraft is subjected to screening for explosives in accordance with a

~~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.~~

robust assortment of Transportation Security Administration (TSA) regulations that were implemented in response to the 9/11 act.

DHS also uses targeting and predictive analysis to identify associated risks with each import, and based on that analysis, the agency selects high-risk shipments for cargo screening and inspection. If selected for inspection, the importer is responsible for presenting the merchandise for examination and paying any associated costs. DHS has undertaken a number of Non-Intrusive Inspection (NII) initiatives (e.g., X-ray and gamma imaging, sensors, video surveillance, and radiation detection devices) to more effectively screen and inspect containers without compromising the flow of legitimate trade into the U.S. economy. Physical unloading and examination of shipments is sometimes necessary based on DHS' risk assessments, in which case CBP or the appropriate Partner Government Agency will conduct the inspection and take appropriate action.

DHS' trade security efforts are not limited to the physical examination of cargo at U.S. ports. DHS also relies on intelligence from a number of its programs to identify high-risk shipments and to better concentrate agency resources:

DHS contributes to the security of the air, land, and sea borders by conducting criminal investigations that prevent fraudulent trade practices and the importation of counterfeit goods. By stopping the organizations that facilitate these crimes, DHS prevents the flow of violative goods and practices from reaching our borders. Recognizing that these goods have the potential to harm the public and jeopardize American businesses, ICE conducts national operations that aim to protect health and safety, secure the global supply chains, and uphold the economy.

2. Trade Facilitation – Facilitating Safe and Legitimate Trade in a Complex Global Trade Environment

To better facilitate trade, DHS established 10 industry-specific Centers of Excellence and Expertise (Centers) within CBP. These Centers strengthen America's economic competitiveness and security through integrated industry knowledge and expertise, innovative trade processing procedures and trend analysis, and strategic and impactful trade enforcement actions. The Centers strengthen partnerships with industry sectors, as well as enable DHS to better work with importers and filers on compliance, detecting anomalies, and other facilitation matters.

On an average day, DHS is responsible for processing approximately $6.7 billion of merchandise, which must undergo the process of being declared in a manifest, classified, appraised, and assigned an admissibility determination based on internal risk-based strategies. DHS has developed and

~~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.~~

deployed an automated system to facilitate the electronic importing and exporting of all goods. ACE the backbone of the U.S. Government's "Single Window" system of imports and exports, transmits the trade industry's import/export data to 47 Partner Government Agencies. Through ACE development, DHS has worked to eliminate manual processing and paper, and to simplify, streamline, and modernize the process of importation.

To assist in the development and implementation of the "Single Window" that streamlines the import/export process for America's businesses, the Border Interagency Executive Council (BIEC) was established and charged with improving coordination among the Partner Government Agencies with import and export requirements. The BIEC is the lead for the One U.S. Government at the Border effort, which is an initiative to enhance interagency coordination and management across the border.

3. Trade Enforcement – Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors

DHS utilizes a proactive, aggressive, and dynamic trade enforcement approach to protect the American people against illicit or fraudulent trade. DHS uses all of its authorities and focuses critical resources to combat trade fraud by detecting high-risk activity, deterring non-compliance, and disrupting fraudulent behavior to ensure U.S. industry can compete on a level playing field.

A variety of tools are used by DHS to execute its trade enforcement approach. To identify violators, DHS uses an integrated targeting approach, which employs a vast network of specialists across the country, and provides targeting and analysis expertise that supports trade compliance, security, and field enforcement operations – including information intake, analysis, targeting, investigative case support, and operational assessments. DHS provides the trade community the opportunity to submit electronic allegations to report violators. The trade remains a crucial partner in DHS' enforcement efforts, providing valuable industry intelligence that can lead to identification of potential high-risk activities and illicit trade.

DHS coordinates with U.S. industries, Partner Government Agencies, and foreign governments to detect anomalies, trends, and violations in the global supply chain to target high-risk shipments and promote compliance. DHS investigates and aggressively seeks prosecution of noncompliant importers, exporters, manufacturers, brokers, counterfeiters, and others who commit related crimes that violate U.S. trade and intellectual property laws and international agreements. DHS conducts criminal investigations of those engaged in, or benefiting from, dumping or receiving foreign government subsidies and countervailing duty investigations of noncompliant importers attempting to circumvent payment of required duties. For example, CBP and ICE collaborate to develop cases, affect civil penalty actions (i.e., monetary fines), and prosecute criminal violations with a range of enforcement actions used to punish criminal violators to the fullest extent of the law. CBP and ICE are also focused on preventing the importation of goods manufactured using forced, child, or convict labor, working with domestic and international stakeholders to ensure importer compliance with this law.

Outreach and training is also an essential component of DHS' enforcement efforts. Through outreach, public engagement, and private/public partnerships with the trade community, DHS raises awareness of the dangers of trade-based violations, and promotes informed compliance, which is the shared responsibility between CBP and the trade community. Through the principle of informed

~~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.~~

compliance, CBP effectively communicates compliance requirements to the trade community so that they may conform to all U.S. trade laws and regulations.

4. Private Sector Engagement

DHS maintains a collaborative relationship with private sector entities and the public, as they play an instrumental role in the global economy and lend their considerable expertise to DHS. Through partnerships with industry leaders, DHS links its processes with modern business practices, which results in enhanced compliance with trade laws and improved DHS facilitation and enforcement efforts. TSA, for example, conducts ongoing engagement with air cargo industry stakeholders in an effort to facilitate continuous enhancement of cargo security measures. A key instrument to DHS' efforts to ensure accurate, timely, and consistent information and to solicit private sector industry feedback is the Commercial Customs Operations Advisory Committee (COAC). The COAC is comprised of private sector members whose operations are affected by the commercial operations of CBP. DHS also works through various informal and formal groups, such as the Trade Support Network, to identify opportunities to provide information to its external stakeholders.

~~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
Travel Security and Facilitation

OVERVIEW

- The Department of Homeland Security (DHS) maintains a high level of security, while facilitating domestic and international travel in the land, air, and sea environments.
- The Transportation Security Administration (TSA) is charged with protecting the nation's transportation systems, and U.S. Customs and Border Protection (CBP) is responsible for ensuring U.S. border security; at the same time, both agency missions seek to ensure the facilitation of legitimate travel.
- The mission of DHS as it relates to security and travel facilitation, has a direct and significant impact on our national security and economic prosperity.
- The travel environment also presents a unique space in which DHS often collaborates with other public and private sector stakeholders to better secure and serve the public; interested and frequently vocal stakeholders in this space, including travelers, industry associations, local partners, and Congress.
- Ultimately, DHS's goal is to provide seamless entry and exit screening, vetting, and verification processes using advanced technologies, such as biometrics, while ensuring U.S. national security and the safety of the traveling public. Key challenges in the security and travel facilitation space include a dynamic threat environment, which consists of:
  - Efforts by terrorists to evade aviation and border security;
  - Increases in the number of individuals requiring access or credentials to critical transportation sectors; and
  - A continuing increase in the number of lawful travelers within and to the United States.
- To meet these challenges, DHS must continue to evolve its security and travel facilitation posture through:
  - Investments in DHS's **targeting, screening, and vetting infrastructure**;
  - Efforts to **identify and interdict potential threats at the earliest possible moment** and prior to departure to or encounter in the United States;
  - The continued development of **business transformation initiatives** that optimize the use of resources;
  - **Joint initiatives** between CBP and TSA for both security and facilitation, and continued advancement of the use of **biometrics** throughout the travel continuum for better security and facilitation.

DETAILED DISCUSSION

Role of DHS in Security and Travel Facilitation

- DHS achieves its multi-faceted mission set, of securing and facilitating travel, through a multi-layered security strategy, which includes the identification of high-risk travelers and targeting of threats before they depart for, fly over, or travel within the United States.
- Through CBP's National Targeting Center (NTC), the National Transportation Vetting Center, Secure Flight vetting, Preclearance, the Immigration Advisory and Joint Security Programs, and Regional Carrier Liaison Groups, DHS works with interagency partners and host governments to identify threats at the earliest possible moment and prior to travel.

~~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.~~

  - CBP's Preclearance program provides DHS's highest capability of border security, placing a highly effective counterterrorism asset, a trained U.S. law enforcement professional, at last points of departure to interdict and address potential threats.
    - Through Preclearance, the same immigration, customs and agriculture inspections of international air passengers performed on arrival in the United States can be completed before departure at foreign airports instead.
    - Currently, Preclearance operations take place at 15 foreign airports in six different countries, benefitting air passengers, airports, and air carriers in the United States and abroad.
- DHS also utilizes targeted enforcement by CBP Agriculture Specialists to prevent the entry of potential threats to U.S. plants and livestock.
- DHS adjudicates agricultural quarantine risks by determining admissibility, evaluating compliance, conducting risk-based targeting, and performing exams of commodities and conveyances.
- DHS also secures and facilitates travel through the vetting of "insider threat" individuals in transportation and recurrent vetting of individuals who apply for, or currently hold, credentials or access to critical transportation sectors.
- DHS coordinates operations across intelligence, law enforcement, and stakeholders to ensure security.
- DHS also employs Trusted Traveler programs and business transformation initiatives that increase security while facilitating legitimate travel.
- DHS Trusted Traveler programs, such as CBP's Global Entry, and TSA Pre✓® Application Programs provide for expedited clearance through CBP inspectional and TSA security screening processes for pre-approved travelers. The results are quicker, more seamless processes for the traveler and less resource intensive inspections for DHS, which allow for the optimized use of resources in support of DHS's security mission.
- Likewise, DHS employs business transformation initiatives for greater efficiency, resulting in a decrease in overall workload requirements, translating to equivalent staffing savings, which may then contribute to more effective security operations. For example, initiatives such as:
  - Automated Passport Control, Mobile Passport Control, and the use of electronic information capture (further reducing the need for paper forms) facilitate the U.S. entry process for the vast majority of travelers applying for admission into the United States;
  - DHS employs Automated Screening Lanes for rapid deployment of passenger and baggage screening technology at airports. Automated screening lanes incorporate technology and screening modifications that enhance security effectiveness while decreasing the time travelers spend in security screening.
- DHS continues to develop biometric entry/exit solutions, in part to meet Congressional mandates for a comprehensive biometric exit validation process, as well as to strengthen the integrity of the U.S. immigration system, and to strengthen identity verification prior to aircraft boarding.
- In the air and sea environments, DHS currently validates and documents departing travelers and matches this data against arrivals to identify visa overstays and enhance our immigration processes.

~~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 is transitioning from field testing experiments to the implementation of a Biometric Exit Program of Record, and is also developing capabilities to validate passenger trusted traveler biometrics at security screening lanes to enhance identity verification and facilitate travel.

Issue Background

- DHS's approach to securing travel has evolved through the use of enhanced detection technologies, new capabilities, and changes in operational procedures, driven primarily by dynamic terrorist threats and an increasing numbers of lawful travelers to and within the United States.
- Terrorists continue to evolve tactics to evade aviation security measures and U.S. entry processes as a means to move operatives into the United States, or to attack the homeland. In FY 2016, the CBP NTC identified and recommended that boarding be denied for over 6,300 potential mala fide travelers; referred over 2,600 visas for visa revocation by the Department of State; and nominated over 3,400 individuals to the Terrorist Screening Database. Similarly, the TSA National Transportation Vetting Center vets approximately 700 million passengers annually prior to arrival for airport screening, and recurrently vets over 17 million individuals with access to transportation sectors, including aviation and port workers.
- The volume of domestic and international travel has continued to increase, the latter rose in all three transportation modes (1.1% in land, 5.1% in air, and 0.4% in sea environments) during FY 2015. During FY 2015, TSA screened approximately 695 million passengers, 1.5 billion carry-on bags, and 450 million checked bags, and discovered thousands of prohibited items (i.e. guns, flammables, knives, etc.) every day at approximately 440 domestic airports. Overall, air passenger volume growth averaged 5% in FY 2015 and is averaging 6.5% for FY 2016. In FY 2015, CBP processed over 112 million arriving international air passengers into the U.S., setting a new all-time record and representing a 5.1% increase over FY 2014 and a 28% increase since FY 2009. Not to be outdone, FY 2016 experienced an additional 6.3% increase over FY 2015.
- Demand for screening and security services, both for international and domestic travel, continues to increase as DHS takes on additional mission requirements, as infrastructure expands, and as trade and travel volumes continue to grow. To meet these growing challenges, DHS has, among other efforts:
  - Developed a Workload Staffing Model to accurately determine officer requirements at each port of entry. Based on most recent calculations, an additional 2,107 CBP Officers and 631 Agriculture Specialists are needed through FY 2017 to meet current work demands.
  - Increased the original FY 2017 Transportation Security Officer requirements by 2,017 to ensure effectiveness and mitigate increased passenger volumes. Additional resources are needed to further mitigate the effects of increased passenger volumes and improve checkpoint performance.
  - Established an Alternative Funding Program, which enables partnerships between CBP and the private sector or government entities, such as the City of Houston Airport System, Denver International Airport, and Miami-Dade County, which allows for additional inspection services on a reimbursable basis upon the stakeholder's request, as well as for

~~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.~~

the receipt of real and personal property donations to enhance U.S. port of entry operations.

Courses of Action

- *Targeting, Screening, and Vetting Infrastructure*:
  - Continue to invest in CBP's NTC, as well as TSA's transportation screening and vetting infrastructure, to further strengthen DHS's robust pre-departure targeting, visa and trusted traveler vetting, data exploitation, information sharing initiatives, and counter network strategy to identify and address threats before they reach U.S. soil and/or board aircraft within or to the United States.
    - Currently, DHS maintains on-the-ground overseas capabilities through Immigration Advisory and Joint Security Programs, or Preclearance facilities, at eight of the top 10 departure points to the United States. The remaining two airports are covered by Regional Carrier Liaison Groups (RCLGs).
    - DHS will continue to build information sharing networks and targeting capabilities, such as CBP's NTC's Automated Targeting System, by cultivating overseas partnerships, which include both foreign governments and private sector entities.
    - DHS is implementing new detection technologies and more thorough procedures to strengthen individual layers in its overall security approach, which includes establishing a unified, intelligence-driven approach to risk management across the domain that links and dynamically uses government and industry security countermeasures, while responding to risk.
  - Continue to invest in vetting, advanced targeting, and screening processes for commercial airline passengers, crew, and individuals who may present an "insider threat," including those requiring access or credentials to secure areas of the transportation sector.
- *Preclearance Expansion*: Continue expanding DHS's Preclearance program, which provides for U.S. immigration, customs, and agriculture inspections, as well as expanded aviation security screening that is comparable to that of U.S. domestic airports at last point of departure airports overseas.
  - On May 29, 2015, the DHS Secretary publicly announced ten airports in nine foreign countries as priorities for preclearance expansion.
    - On November 4, 2016 the U.S and Sweden signed an agreement to implement preclearance at Stockholm Arlanda Airport (ARN). The agreement must now be brought into force after the Governments have completed all necessary internal procedures. This process is expected to take between 12 and 18 months.
    - CBP also expects to sign an agreement with the Dominican Republic for preclearance operations at Punta Cana Airport (PUJ) before the end of calendar year 2016. Preclearance operations at PUJ are expected to begin in late 2017.
  - In May 2016, DHS announced a second Preclearance expansion open season which closed on August 1, 2016. DHS received 21 letters of interest. On November 4, 2016 the DHS Secretary announced 11 new preclearance expansion airports in 9 countries.
- *Business Transformation Initiatives*: Continue to develop and implement business transformation initiatives across DHS to more effectively utilize resources, maintain security, and facilitate legitimate travel into and within the United States. In addition to Automated and Mobile Passport Control, DHS maximizes resources and transforms the way travelers visit and

~~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.~~

transit through the United States through programs such as CBP Mobile, Ready Lanes, the Electronic System for Travel Authorization (ESTA), the Electronic Visa Update System (EVUS), as well as TSA's Innovation Task Force airport security initiatives such as Automated Screening Lanes, Credential Authentication Technology, and Biometric Authentication projects. For CBP, business transformation initiatives comprise one part of CBP's three-part Resource Optimization Strategy; the other two parts include: 1) utilizing CBP's workload staffing model to accurately and transparently identify staffing needs at a port-by-port basis, and 2) cultivating public-private partnerships to support growing volumes of trade and travel.

- *Joint Initiatives*: Foster ongoing joint initiatives between CBP and TSA to facilitate travel and advance intelligence and operational awareness. Significant opportunities exist for DHS components, like CBP and TSA, to partner in developing operational requirements, such as biometric identity validation, as well as in leveraging CBP and TSA's established network of information sharing, vetting capabilities, and domestic/foreign partnerships.
- *Biometrics*: Continue to develop the use of biometrics and implement those technologies throughout the travel continuum (from airline check-in, to transportation security screening, to international arrivals at a port of entry) to strengthen the U.S. travel and immigration systems. Biometric technologies can provide security and facilitation benefits, including confirming the entry and exit of a traveler, closing security gaps in the facilitation of travelers and identity verification, and allowing for greater automated processing and facilitation.

Key Partnerships

- DHS has a wide-variety of partners and stakeholders with whom it collaborates on policy, security, and facilitation efforts.
- The travel environment is unique for DHS, given physical presence and operations in locations shared with other public and private sector stakeholders, such as airport authorities, local municipalities, state and local law enforcement, and international partners
- DHS enforces more than 400 laws for more than 60 Federal agencies and works with a number of federal partners.
- With a mission to facilitate legitimate travel, DHS collaborates with a range of public and private sector stakeholders including:
  - Federal, state and local stakeholders;
  - Industry; and non-governmental organizations on travel and tourism related matters including security, facilities, staffing levels, and customer service; and
  - Non-governmental organizations also engage DHS on privacy and civil rights/liberties issues.
- At the international level, DHS engages with foreign governments, organizations, and law enforcement in setting international policy and agreements regarding aviation security, harmonizing customs laws, and collaborating on security-related issues and information sharing.

~~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.~~

TRANSPORTATION SECURITY ADMINISTRATION

TSA Brief

Agency Review

Huban A. Gowadia, PhD
TSA Deputy Administrator

★ ★ ★ ★ ★ ★

December 13, 2016

Non-Disclosure Agreement

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

- TSA's Operational Environment – Balancing security and facilitating tradeInnovation – Evolving the Transportation Security EnterprisePeople - Recruiting, Incentivizing and Retaining a World Class Workforce Training - Creating a Professional Counterterrorism ForceEquipment and Technology - Facilitating Mission SuccessPartnerships – Promoting Internal and External Collaboration

TSA's Operational Environment

Persistent Threat

Adversaries are **evolving more quickly** and are using variants of previously seen tactics.

Security & Trade Facilitation

Last year, aviation **passenger growth** was 6.2% over 2015. Expecting 4-7% growth in 2017.

Globalization

With a global threat and a global system, we must act on a global level

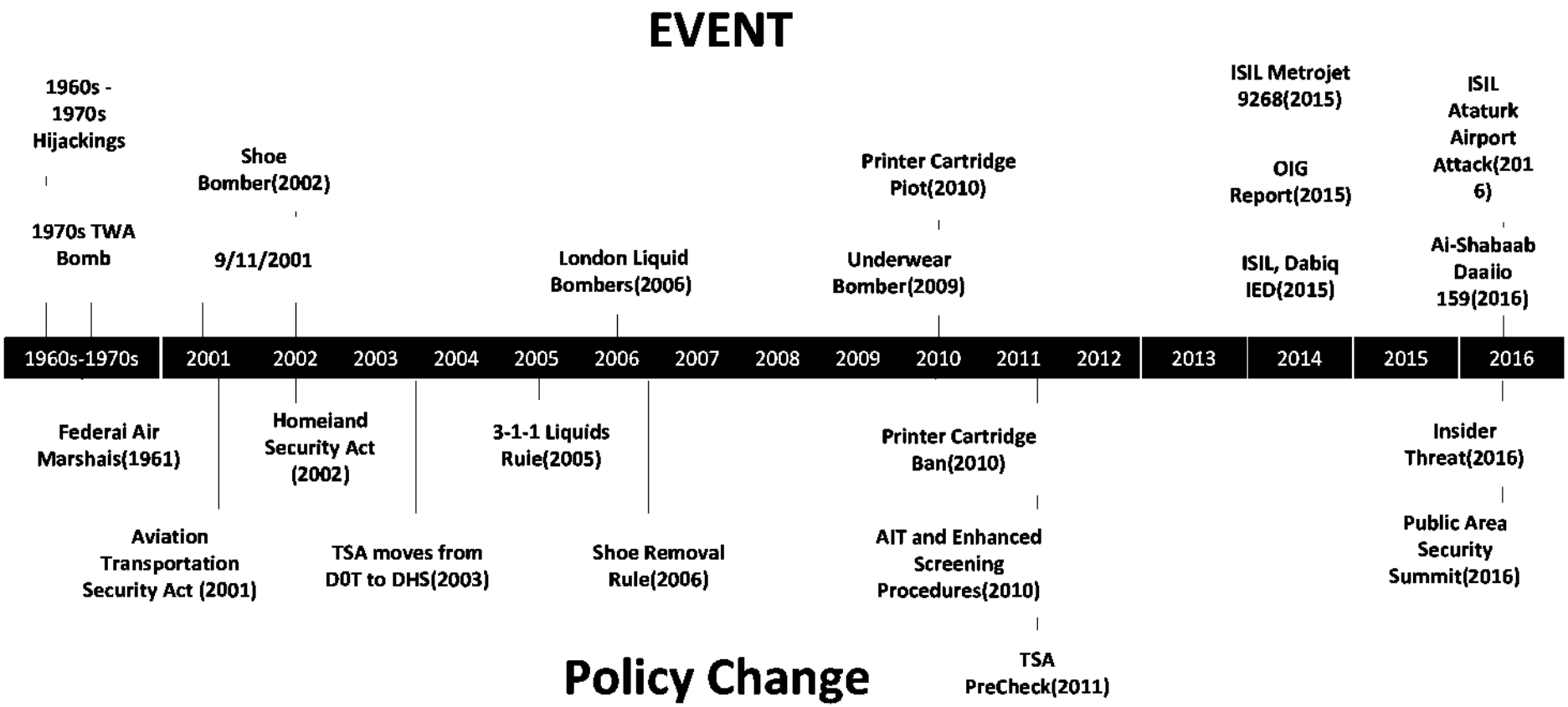
Intermodal

Adversaries are targeting modes of transportation **outside aviation.**

Interconnected systems are becoming increasingly vulnerable to **cybersecurity** threats.

Scale and Volume (Annually)~740 Million passengers screened at 450 domestic airports18.5 Million flights by general aviation pilots~260-280 airports providing last point of departure service to the U.S.15 Million tons of air cargo shipped each day by 4,000 freight forwarders75% of U.S. crude oil transported by pipelines2.7 Million miles of gas distribution pipelines2.8 Million car loads of freight moved over 140,000 miles of freight rail track10.7 Billion trips by mass transit and passenger rail system users4 Million miles of roads including 11,500 miles of freeways and expresswaysEconomic Impact (Annually)12 Million jobs related to the transportation sector$18 Trillion annual value of goods movedContributes 8.6% to the gross domestic product

Key Aviation Events and Policy Changes



A dynamic and persistent threat which can be inspired, enabled, or directed, will continue to target the transportation system

Innovation

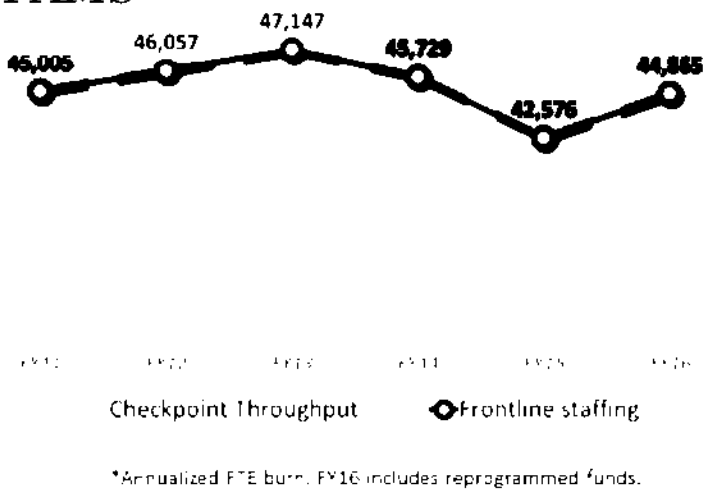
- Innovation in all things – equipment, training, policies and personnel managementThinking and designing in terms of security environment with all security partnersWeaving security into the very fabric of aviationThinking beyond airport perimeters, public areas, checkpoints, and sterile areas towards a "reservation-to-destination" concept

Require technologies at the "speed of the threat" to address existing gaps and improve the passenger experience

People

55,590 FTE*	44,865 screening FTE

- Annualizing workforce Full Time EmployeesAttrition Federal Employee Viewpoint Survey resultsUnionized Transportation Security Officer workforce Collective Bargaining Agreement41,517 bargaining unit employeesDues are optionalNo Title 5Administrator's Determination*Excludes FAMS



Scale the workforce in alignment with threat, technology, and passenger volume

Training

- **Transportation Security Officer (TSO) TrainingTSA Academy trains up to 10,000 new hires annuallyDedicated classroom & training facilities Explosive Detection Canine Training Trained 230 canine teams in FY16, with ~300 projected for FY17Leadership Training In 2016, TSA created it's first Transportation Security Leadership Development ProgramRising Leader Development ProgramMid-level Leader Development ProgramSenior Leader Development ProgramNational Preparedness Leadership Initiative Mandatory training for newly promoted J and K band supervisors is being implemented in 2017**

Build a foundational culture and improve performance by standardizing training for TSA at all levels

Equipment and Technology

- Require technologies at the “speed of the threat”Develop and deliver solutions to implement “reservation-to-destination” securityInterconnect aviation screening equipmentPilot use of artificial intelligence capabilitiesBuild and deploy a more robust canine cadreEngage private sector, e.g. through the Innovation Task ForceImplement acquisition reform to allow for disciplined decision-making

Acquire and deploy capabilities that advance and strengthen the nation’s transportation security system

Partnerships

Key Stakeholders and Associations

Commercial Airlines

- Security Directors at Major Airlines
- Airlines for America (A4A)
- Regional Airline Association (RAA)
- International Air Transport Association (IATA)
- National Air Carrier Association (NACA)

Commercial Airports

- Airport Security Coordinators at Major U.S. Airports
- American Association of Airport Executives (AAAE)
- Airports Council International (ACI)
- Airport Consultants Council (ACC)
- Airport Law Enforcement Agencies Network (ALEAN)

Air Cargo (Air Operations)

- Major passenger airline and all cargo airline Security Directors
- Cargo Airline Association (CAA)
- Express Association of America (EAA)
- The International Air Cargo Association (TIACA)

Air Cargo (Surface Operations)

- Air Forwarders Association (AFA)
- Express Delivery and Logistics Association (XLA)
- International Air Transport Association/ Cargo Network Services (IATA/CNS)

General Aviation

- National Business Aviation Association (NBAA)
- Aircraft Owners and Pilots Association (AOPA)
- National Air Transport Association (NATA)
- General Aviation Manufacturers Association (GAMA)

Interagency Liaison

- The Aviation Government Coordinating Council (AGCC)
- Aviation Sector Coordinating Council (ASCC)
- Aviation Security Advisory Committee (ASAC)
- Aviation Domain Intelligence-Integration Analysis Cell (ADIAC)

Other Stakeholders

- Coalition of Airline Pilots Association (CAPA)
- Airline Pilots Association (ALPA)
- Association of Flight Attendants (AFA)
- National Association of State Aviation Officials (NASAO)
- National Laboratories
- Universities and Centers of Excellence

Cultivate and advance partnerships with stakeholders across the transportation security ecosystem

On the Horizon

- DHS Inspector General is conducting the next round of covert testingTSA will provide support to the USSS for the InaugurationWe must continue to address growth in aviation Spring break travel volumeTSA will advance global standards and capacity building through international partnerships and implementation of UNSCR 2309

Transportation Security Administration

The Transportation Security Administration protects the Nation's transportation systems to ensure freedom of movement for people and commerce.