Transportation Security Administration

Office of Security Capabilities Cybersecurity Plan

Version 1.1

August 10, 2015

The contents of this plan draw from, and are in alignment with, requirements identified in existing National Institute for Standards and Technology, Department of Homeland Security, and Transportation Security Administration (TSA) policies, as well as the Office of Security Capabilities Cybersecurity Management Framework. This plan is not intended to supersede any existing compliance-related policy enforced by the TSA Office of Information Technology. Additionally, this plan may be adapted or updated as necessary based on changing requirements, guidance, policies, and procedures.

Table of Contents

Executive Summary

The Transportation Security Administration's (TSA) Office of Security Capabilities (OSC) is responsible for identifying, testing, procuring, and deploying transportation security equipment (TSE) to protect the American aviation system. OSC holds the primary responsibility for securing TSE, which includes applying cybersecurity mechanisms to the environment. Given today's increasingly prevalent cyber threats, unprotected TSE may fall victim to a cybersecurity breach and yield potentially deadly consequences. As a result, OSC developed a cybersecurity plan that protects OSC's most sensitive and mission critical data and systems and complies with federal requirements.

To create this plan, OSC solicited input from its internal and external stakeholders; analyzed cybersecurity guidance, policy, and best practices, such as those distributed by the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS); and leveraged the OSC Cybersecurity Management Framework. The plan creates a risk-based cybersecurity regime that dynamically responds to new technologies, threats, and required compliance actions. It is characterized by a defense-in-depth security architecture, continuous cybersecurity monitoring, and enhanced operational capabilities to maintain a technology environment. The four goals that enable OSC to realize of this future state are:

- **Goal 1:** Apply continuous monitoring processes to the environment for security weaknesses and prioritize remediation efforts;
- **Goal 2:** Use sound security processes to mitigate known and existing cyber vulnerabilities;
- **Goal 3:** Acquire, develop, and test technologies that lower cybersecurity risk; and
- **Goal 4:** Assign and enforce responsibility to comply with policy and standards.

Each goal is supported by specific activities and low, medium, and high maturity subtasks necessary to execute the goals and achieve OSC's desired end-state.

Of these activities and tasks, the OSC prioritized the following five items to secure TSE and comply with emerging government requirements:

- **Asset Inventory:** Underpins the transition to a mature cybersecurity capability, including asset prioritization, discovery scanning, vulnerability scanning, threat assessments, operating system patching, antivirus updates, and locating and updating obsolete and unsupported operating systems.
- **Basic Discovery Scanning:** Related to asset inventory, enables OSC to confirm its existing inventory and is required for the *Federal Information Security Modernization Act* and continuous diagnostic and mitigation compliance.
- **Asset Risk Prioritization:** Helps OSC determine how to apply cybersecurity resources to safeguard its most important data and systems, while simultaneously meeting requirements of the government's Cyber Sprint and creating long-term resource optimization.
- **Design Standards for Imminent Procurements to Support Recapitalization:** Helps vendors plan for new TSE cybersecurity requirements.
- **Full Lifecycle Planning:** Completes transition planning for the remainder of the plan implementation over the next several years, including assigning resources and organizational responsibilities for plan implementation.

This plan matures OSC into a state of compliance and proactivity against cyberattacks on mission-critical information technology systems. The plan will be updated based on a changing threat landscape, guidelines, and requirements, and is not intended to replace existing compliance or policy enforced by TSA or other government bodies.

1 OSC Background and Introduction

The Transportation Security Administration's (TSA) Office of Security Capabilities (OSC) is responsible for implementing advanced security solutions to protect the American aviation system, ensuring freedom of movement for people and commerce across 440 airports around the country and screening over 1.8 million passengers each day. OSC identifies, tests, procures, deploys, and maintains transportation security equipment (TSE) that is capable of detecting threats concealed on passengers and in their baggage. Since OSC holds primary responsibility for securing TSE, it is also responsible for the cybersecurity mechanisms applied to the environment.

2 Cyber Threat Environment

Organizations across government and industry are grappling with increasingly skilled adversaries operating within a dynamic cyber threat environment. These actors have precipitated a significant increase in the number and intensity of cyberattacks targeted at stealing confidential information, compromising user actions, or disrupting service for a target agency. As evidenced by recent high-profile breaches and cybersecurity's prominence in the Department of Homeland Security's (DHS) *2014 Quadrennial Homeland Security Review*, cyberattacks are the next frontier of threats faced by federal agencies and warrant the same urgency as other mission threats.[1]

In parallel, OSC is in the process of creating the airport of the future through a more interconnected screening technology environment. With increased connectivity, TSA can realize a multitude of benefits that propel it to become a more advanced, dynamic, and data-driven agency; however, this increased connectivity comes with an increased risk of compromise. The implementation of strong, layered security capabilities is more important than ever in this evolving cyber threat landscape. In this new paradigm, cyber compromise could lead to either relatively minor disruptions (e.g., defacing a public-facing website) to loss of life (e.g., disabling the explosive-detecting capability of TSE without triggering an alarm). These potential scenarios represent the new normal for OSC as the technology that underpins TSA's mission continues to advance.

3 Purpose of the OSC Cybersecurity Plan

With a rapidly evolving technology and cybersecurity threat environment, OSC recognized the need to implement preventative measures to lower the risks associated with the compromise of TSE. This Cybersecurity Plan aims to provide discrete, actionable steps that OSC will take to safeguard the technology, data, and people that its mission supports on a daily basis. Specifically, this plan:

- Articulates the existing cyber threats and vulnerabilities of TSE to government and industry stakeholders;
- Communicates the goals, activities, and subtasks that mitigate the threats and vulnerabilities;
- Correlates existing capabilities with organizational cyber goals to bring OSC into compliance with DHS FISMA cybersecurity and other escalated metrics released by the Federal Chief Information Officer in a cost-effective manner and lays the groundwork for the future acquisition of more secure cyber capabilities; and
- Evolves and adjusts over time to respond to the dynamic nature of cyber threats and new guidance published by the Executive Branch and DHS leadership.

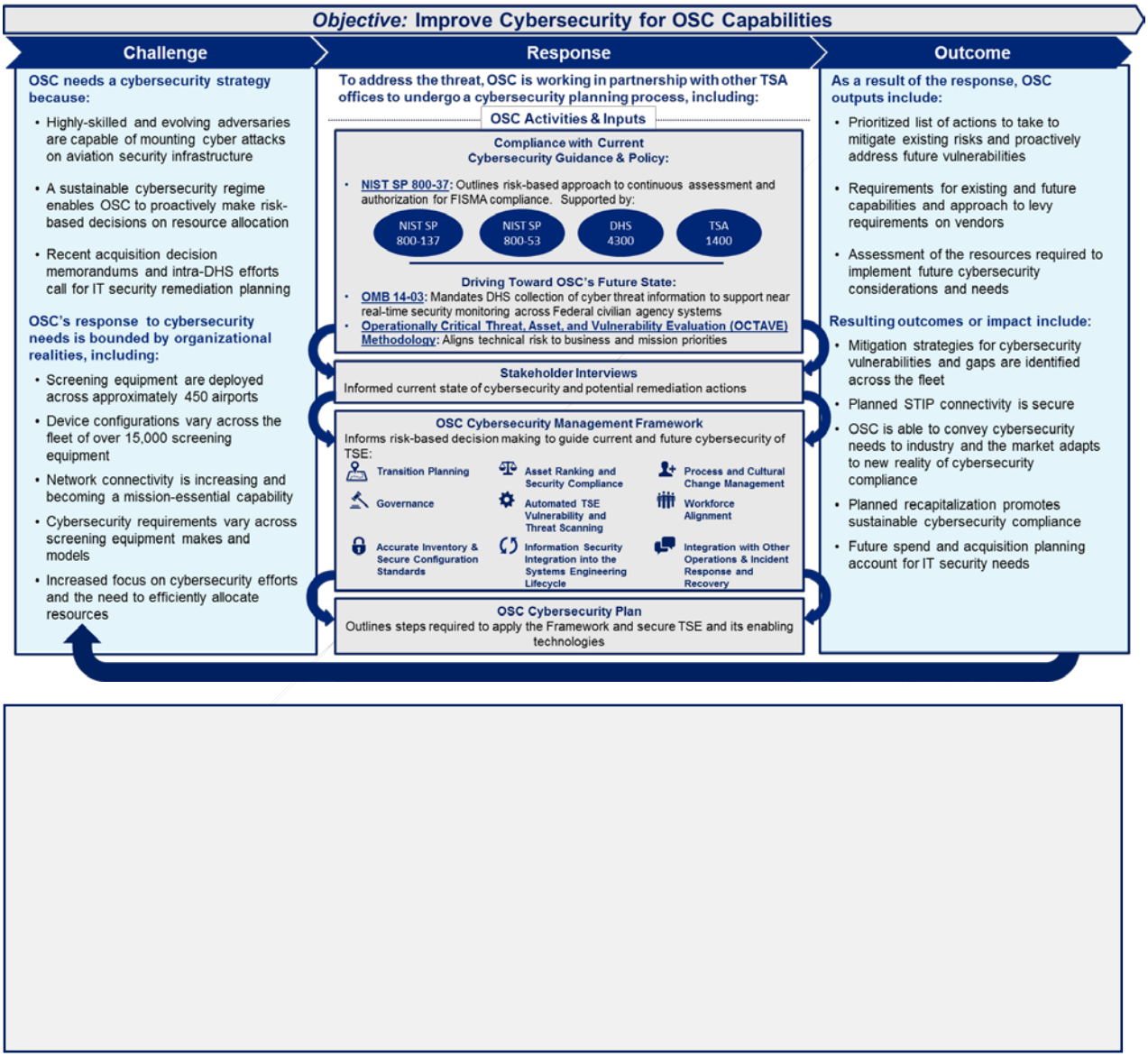
The OSC Cybersecurity Plan draws from strategic goals from a variety of planning documents, discussions from a joint cybersecurity planning session between OSC and the TSA Office of Information

[1] DHS. *2014 Quadrennial Homeland Security Review*. June 2014. http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

Technology (OIT) in April 2015, and interviews with 22 stakeholders across its organization and its partners.[2]

The OSC Cybersecurity Plan was also developed based on the OSC Cybersecurity Management Framework. The framework organizes the lifecycle of security considerations for which OSC accounts and provides OSC leaders with an adaptable risk-based model to address cybersecurity vulnerabilities. It includes nine elements that encompass processes and procedures to identify and manage cybersecurity risks across technical, operation, and policy fields.[3] The nine elements come together in this OSC Cybersecurity Plan to provide an assessment of OSC's current cybersecurity posture; establish the desired end-state for OSC cybersecurity; and establish specific goals, activities, and subtasks that OSC will implement to close the gaps between current and end-state environments. Figure 1 depicts how the current operational environment, regulatory requirements, and Cybersecurity Management Framework's elements come together to drive outcomes of the OSC Cybersecurity Plan.

Figure 1: OSC Cybersecurity Management Framework Overview



[2] Reference Appendices B and C for more information on the development of this plan.
[3] Reference Appendix A for additional details on the OSC Cybersecurity Management Framework.

4 Current State of Cybersecurity for TSE

TSA's current security technology profile, designed to screen both passengers and their baggage, includes approximately 15,000 total pieces of deployed TSE, representing more than 45 different models developed by more than 10 different vendors. The highly-customized configuration nature of TSE, coupled with their geographically-distributed locations, makes enterprise management difficult from a security perspective. Maintaining a secure configuration on each TSE requires substantial time and resources; therefore, security controls for TSE are only reviewed and updated every three years. Furthermore, only a small percentage of TSE are network-enabled, further complicating the timely analysis of security configurations present on TSE after they are deployed at airports.

4.1 Understanding Connectivity – The Security Technology Integrated Program

To establish connectivity, OSC's screening programs, the Electronic Baggage Screening Program and the Passenger Screening Program, rely on the Security Technology Integrated Program (STIP). STIP is an information technology (IT) program, classified as a High Impact System under the *Federal Information Security and Modernization Act* (FISMA) that connects all TSE to a single logical network using existing TSA network infrastructure, enabling automated two-way information exchange.

STIP enables centralized management and monitoring of the TSE fleet and provides the ability to respond to the rapidly changing threat environment in a more agile manner. STIP meets information collection, retrieval, and dissemination requirements of the screening programs, and addresses potential areas of improvement within operations and maintenance for TSE. STIP's benefits are realized as it is rolled out to more pieces of TSE, though currently, only network-enabled TSE can leverage STIP.

4.2 Safeguarding TSE

Current challenges to TSE cybersecurity efforts include conducting timely scanning and maintaining compliance with guidelines and standard operating procedures (SOP), mandating IT security requirements for vendors, securing external interfaces, coordinating access control, and securing TSE's physical environment. OSC has taken steps to identify and implement IT security controls and position OSC for future defense against cybersecurity attacks. These efforts include:

- **Supported Operating Systems (OS):** In April 2015, OSC began efforts to catalogue and disconnect any TSE that was not running a supported OS. Currently, OSC has made progress to replace outdated Windows operating systems and will continue its effort until all TSE run on a supported OS.
- **Patching Process:** The specific nature of TSEs require them to be tested for OS patch compatibility before the patches are pushed out, and such patches can only be done by vendors due to the proprietary nature of their systems. Keeping these constraints in mind, STIP and OIT's Operations and Engineering Division have developed a process map to remotely patch CAT machines that can serve as a blueprint for other TSEs.
- **Anti-Virus (AV):** AV protections are currently outdated for connected and non-connected TSE, due to the labor-intensive process required for manual updates. OSC is working to push anti-virus updates in real time to all TSE, regardless of connectivity.
- **Vendor Cybersecurity Requirements:** OSC developed an information assurance (IA) technical guidance package and statement of work (SOW) to detail cybersecurity requirements for TSE in collaboration with OIT's Information Assurance and Cybersecurity Division (IAD). The SOW details cybersecurity requirements that impact existing and future contracts. High-level requirements provide support for AV software, operating system patching, hardening, technical obsolescence, security scanning, and plans of actions and milestones (POA&M) remediation.
- **Define and Baseline OSC Security Architecture:** OSC continues to define capabilities as part of a broader system architecture, which requires it to define an associated security architecture.

Components of this security architecture include network security controls, such as VLAN separation, Transport Layer Security encryption (FIPS compliant), and port security. The security of the embedded software of the TSE itself.

- **STIP Authority to Operate (ATO) Renewal:** As part of the ATO renewal, OSC developed a strategy to assess TSE as part of the STIP boundary. A requirement for maintaining the ATO is to assess TSE on a recurring basis; however, the size and complexity of the STIP system boundary, which contains the entire TSE fleet, as well as the resources needed to support scanning, makes it difficult to do.
- **Physical Security:** OSC published guiding documentation with physical security controls for TSE; however, continued coordination with airports and the Transportation Security Officer (TSO) workforce is needed to control access and see that standard operating procedures and similar policies are enforced at the operational level.
- **Vulnerability Assessments of TSE:** These assessments help shape OSC's current IT risk management approach. The passenger and baggage screening programs are working with vendors, national labs, and universities to conduct IT security threat and gap analyses.

5 Desired Cybersecurity Posture

To enhance the effectiveness of OSC's mission and position itself to operate in the evolving threat environment, OSC requires a future state that enables a risk-based cybersecurity regime that is flexible and adaptable to new technologies and threats. OSC also needs to comply with mandatory security regulations and DHS policy guidance.[4] This cybersecurity end state for OSC, characterized by a defense-in-depth security architecture, continuous cybersecurity monitoring, and enhanced operational capabilities targeted at maintaining a secure technology environment, includes the following elements:

- Full connectivity of all TSE, enabling two-way data communication;
- Automation of alerts, scans, and patches to comply with OMB M-14-03 (November 18, 2013) on continuous diagnostics and mitigation;[5]
- Advanced data encryption standards and access control processes;
- Cybersecurity incorporated into the development and design of future capabilities, instead of being applied retroactively;
- A workforce that understands and supports the importance of cybersecurity and how it enhances mission effectiveness;
- Streamlined cybersecurity configuration management processes; and
- Clearly defined roles, responsibilities, and processes for ongoing and effective collaboration with partners.

Achievement of the future state vision secures TSE from cyberattacks and highlights cybersecurity as critical to mission effectiveness.

[4] Reference Appendix B for additional details on the OSC Cybersecurity Management Framework.
[5] OMB M-14-03, *Enhancing the Security of Federal Information Systems*. November 18, 2013. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

6 OSC Cybersecurity Plan

When analyzed in conjunction with mandatory regulatory activities and industry best practices, OSC developed four overarching goals to position itself for long-term cyber health:

- **Goal 1:** Apply continuous monitoring processes to the environment for security weaknesses and prioritize remediation efforts;
- **Goal 2:** Use comprehensive security processes to mitigate existing cyber vulnerabilities;
- **Goal 3:** Acquire, develop, and test technologies that lower cybersecurity risk; and
- **Goal 4:** Assign and enforce responsibility to comply with policy and standards.

These four goals, supporting activities, and corresponding subtasks help OSC achieve its future state by identifying the policies, procedures, and technological advancements necessary to design, implement, and socialize a cybersecurity program of this complexity and scope. The goals address mission critical activities while outlining immediate remediation activities for known vulnerabilities and weaknesses, such as those related to access control and obsolete operating systems.

The goals are highly interdependent and the implementation of each goal is necessary if OSC is to achieve a robust, risk-based cybersecurity posture. For example, without the workforce alignment and training called for in Goal 4, *Assign and Enforce Responsibility to Comply with Policy and Standards*, OSC does not have the necessary staff to support the activities in Goals 1-3. To advance execution of the plan and framework, OSC must collaborate with its partners in OIT, the Office of Security Operations (OSO), the Office of Training and Workforce Engagement (OTWE), and the Office of Acquisitions (OA).

Each goal is supported by several specific activities and subtasks. While there is flexibility in the activities that OSC implements first, the subtasks are meant to be implemented sequentially and are categorized as low, medium, or high maturity. The maturity levels describe an increasing degree of sophistication in cybersecurity risk management practices. Specifically:

- **Low maturity:** Subtasks support basic risk management practices for cybersecurity.
- **Medium maturity:** Subtasks support repeatable cybersecurity processes that are in place and formally recognized across OSC and TSA.
- **High maturity:** Subtasks allow OSC to proactively identify and mitigate threats, as well as adapt to address evolving threats.

For example, the subtasks listed as low maturity are implemented before those listed as medium maturity or high maturity; likewise, both low and medium maturity level subtasks are completed before high maturity subtasks can begin. Success for this plan is defined by the realization of the low, medium, and high maturity tasks within organizationally-appropriate timeframes. Specialized success measures and metrics may be drafted upon assignment of ownership. (See Section 8, *Plan Execution*, for additional detail.)

6.1 Goal 1: Apply Continuous Monitoring Processes to the Environment for Security Weaknesses and Prioritize Remediation Efforts

This goal promotes technology and infrastructure to scan TSE, identify vulnerabilities, and assign action to remediate compliance issues. This goal also includes activities that help inventory and categorize TSA's assets according to risk level, as an accurate inventory count enables more effective monitoring.

Goal 1 champions and facilitates the implementation of automated monitoring techniques like DHS' CDM program. In combination with the automated patching and alerting programs, this enables a future state that is proactive in nature and has the ability to automatically respond to identified threats through security policies, procedures, and software.[6]

Goal 1 Framework Elements Applied:

- Accurate Inventory & Configuration Standards
- Asset Ranking and Prioritization
- Automated Vulnerability and Threat Scanning
- Systems Engineering Lifecycle (SELC) Integration
- Integration with Other Operations and Incident Response

6.1.1 Activity: Asset Inventory

Description and Benefit: The need for an accurate inventory for TSE is critical if OSC is to achieve its goal of near 100% network-connected TSE. TSA's goal to automate data collection of TSE's performance data and equipment status information reduces reporting errors, misallocation of resources, and assets left vulnerable to multiple attack vectors. An understanding of the systems, resources, hardware, and software that support TSE, along with an understanding of how they support OSC's mission, allows OSC and TSA to create risk profiles and prioritize their highest-risk assets.

Activity Subtasks: OSC's current asset and enterprise management solutions that track TSE are:

- The Sunflower Asset Management System (SAMS), TSA's official system of record for accountable property;
- The Government Property Management (GPM) database, a centralized database that stores asset data for every piece of procured TSE; and
- STIP, the IT program that allows STIP-enabled TSE to provide two-way exchange of information.

OSC must continue to use and augment these tools to enable OSC to fully understand its TSE inventory and any inventory gaps. Full maturity also requires OSC to develop processes to guarantee asset inventory is updated in real-time, which allows OSC to map TSE to business and mission functions, therefore having the right cybersecurity protections applied immediately upon introduction.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Upgrade the current processes and tools (e.g., SAMS and the GPM database) used to track inventory • Assess validity of data and any data gaps	• Leverage networked capabilities to map physical and logical asset lists • Automate data collection of TSE performance data and equipment status • Enable database access for inventory processing, analysis, and management decision support • Enable enterprise management functionalities for TSE remote access, system administration, reporting, and system interfaces • Enable configuration management functionality	• Map the assets to higher tiered mission functions of TSE • Enable sustainment functionality of TSE to include remote maintenance diagnostics and repairs

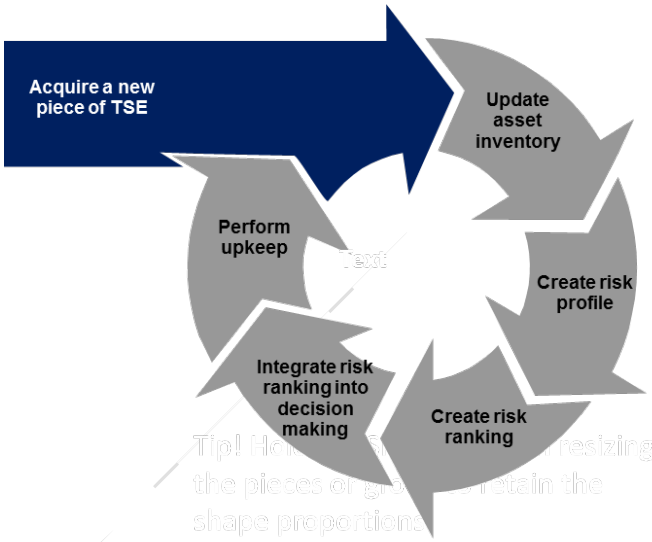
[6] See Appendix B for additional CDM reference.

6.1.2 Activity: Asset Prioritization

Description and Benefit: NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, helped shift security programs to a newer, more effective paradigm where IT assets are differentiated primarily on risk posture.[7] Asset prioritization is the process of determining the highest-risk assets by evaluating both the business process factors affecting an asset as well as the technical factors that drive cybersecurity vulnerabilities.

Activity Subtasks: Fully accounting for required security controls, OSC's current methodology facilitates risk ranking by assigning risk scores to individual security controls that reflect the different levels of threat and vulnerability present within an IT system. With that model comes the challenge of consistently representing risk, understanding all of the underlying factors that could potentially affect a system, and establishing a degree of consistency for the model's application across a diverse and expansive enterprise. This helps shift security efforts from a compliance-based strategy to a risk-based strategy. Additionally, as OSC acquires, inventories, and prioritizes new assets, it will update the asset inventory and create risk profiles to prioritize TSE, as depicted in Figure 2.

Figure 2: Assigning Risk to New TSE



OSC must create individual Component Risk Profiles for each piece of TSE by analyzing the business process and technical factors and generating a quantitative risk ranking from these analyses. This profile represents the rolled up risk ranking for TSE.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Assess current checkpoint operations, technical systems, and threat environment (e.g., through Johns Hopkins University [JHU]) to create component risk profiles	• Integrate findings from JHU threat environment study • Rank and prioritize risk profiles	• Understand how the asset impacts interconnected missions and data flow throughout the environment

6.1.3 Activity: Technical Threat Scanning & Endpoint Monitoring

Description and Benefit: Scanning and monitoring allows an enterprise to identify extant vulnerabilities in the enterprise and categorize them according to risk profiles previously set during asset prioritization. Full operational maturity requires OSC to transition from reliance on labor-intensive, manual assessment policies to a fully-automated capability that supports near real-time data capture. Furthermore, technical threat scanning and endpoint monitoring is required for OSC to fully implement OMB's CDM mandate.

Activity Subtasks: Due to the complexity and size of the network boundary, scanning TSE is currently resource intensive for OIT IAD to support the STIP ATO, as it requires a technician to manually scan and collect data from each piece of connected TSE at every federalized airport across the country. Compliance scanning of various TSE during testing and post-configuration changes is also costly. By leveraging existing tools and incorporating new capabilities provided by OIT, OSC supports a best-of-breed automated assessment infrastructure capable of identifying security vulnerabilities and misconfigurations in near real-time.

[7] This policy is currently driving many of the compliance activities supported by OIT.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Work with OIT to determine process for periodic scanning for STIP-enabled devices • Conduct endpoint monitoring via the TSA Security Operations Center (SOC) • Add engineering service hours to contracts to support scans • Install CDM software on TSE (either TSA or vendor)	• Implement Phase 1 CDM on server platform targets	• Extend the CDM program to integrated hardware and integrated operating system environments

6.1.4 Activity: Audits

Description and Benefit: Strong physical security measures, to include OIG and IAD audits, are critical to properly protecting TSE from malicious or negligent (e.g., human error) activities. Physical security audits are conducted by OSC to confirm that airports are appropriately implementing physical security measures.

Activity Subtasks: Currently, OSC initially issues limited guidelines for physical security through the *Planning Guidelines and Design Standards* (PGDS) and the *Checkpoint Design Guide* (CDG); however, OSC's resources only permit it to conduct 2-3 design audits each year. OSC can streamline its resources by automating the threat scanning and asset inventory processes, thereby enabling the reallocation of those resources for airport audits to further enhance physical cybersecurity.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Create process to establish physical security audits	• Conduct routine and random audits to drive compliance with guidance and SOPs	• N/A

6.1.5 Activity: Incident Response Planning

Description and Benefit: An objective of the recent draft OMB cybersecurity guidance is to strengthen agencies' ability to rapidly respond to cyber threats and incorporate lessons learned from these events into its protocols. As a result, OSC requires a plan to address cybersecurity breaches from hackers, terrorists, and foreign governments while still maintaining critical OSC operations.

Activity Subtasks: Currently, OSC officials work with the OIT SOC and other partners to identify potential direct threats to TSE. As informed by the SOC, OSC must also define how it would continue to operate and allow travel in the event of a catastrophic TSE cyberattack, and how it would respond. This planning is facilitated through exercises. Finally, to fully comply with draft OMB cybersecurity guidance, OSC needs to update its emergency protocols with lessons learned from the exercises.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Plan to conduct incident response planning	• Coordinate with SOC and Network Operations Center to circulate mitigation procedures	• Conduct incident response planning exercises • Incorporate lessons learned

6.2 Goal 2: Use Comprehensive Security Processes to Mitigate Existing Cyber Vulnerabilities

This goal defines a plan for OSC cybersecurity and addresses the creation and enhancement of policies architected and designed to protect assets from threats by internal and external actors. In the low maturity state, these policies and procedures leverage technologies like data encryption, access control, and anti-virus software to remediate vulnerabilities that are identified through scanning procedures. As the organization continues to mature, OSC utilizes automation techniques to increase efficiency and effectiveness.

Goal 2 prompts the creation of tools that are critical to the realization of the desired end-state. It also champions the automation of these tools in high maturity states. This allows for high levels of automated decision making and expedited data collection around vulnerabilities and means for remediation.

Goal 2 Framework Elements Applied:
- Governance
- SELC Integration
- Automated Vulnerability and Threat Scanning
- Integration with Other Operations and Incident Response

6.2.1 Activity: Operating System Patching

Description and Benefit: Patching operating systems to mitigate and protect against potential vulnerabilities is a critical component of cyber hygiene and has recently become a major focus across the government. While proposed guidance from OMB mandates that all agencies patch critical vulnerabilities within 30 days, current OIT requirements are even stricter: for critical alerts, OIT must acknowledge, test, and push out the patch within five business days.

Activity Subtasks: It is important for OSC to first understand its current patching processes and determine a feasible patching cadence, given the uniqueness of mission and drive for automation. Once that is determined, OSC will be able to move toward an automated patching processes and understand how TSE might be impacted if a patch is not immediately applied.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
TSE • Understand current state patching cadence; • Verify consolidated list of missing patches; and • Agree on minimum patch cycles for non-critical vulnerabilities (30 days minimum for critical vulnerabilities) *Servers* • Migrate STIP servers in Data Center to OIT patch management program	• Install endpoint management software on TSE to monitor cyber hygiene • Formalize process by which to notify, evaluate, and deploy OS patches on a routine basis (e.g., process used for Credential Authentication Technology)	• Automate patching. • Understand, identify, and monitor the vulnerabilities caused by a missing OS patch

6.2.2 Activity: Anti-Virus

Description and Benefit: NIST and DHS policy mandates certain requirements around AV software scans that rid a computer of viruses, specifically requiring all machines to have current AV protection prior to connecting to the network.[8] Further, all machines are required to receive AV updates in near-real time and machines with detected viruses are removed from the network while remediation efforts are performed.

Activity Subtasks: OSC currently uses approved AV software with real-time updates on STIP-enabled and connected devices; therefore, unconnected TSE are not updated as frequently as needed to protect against insider threats and other user error that might introduce a virus (e.g., unapproved thumb drive).

[8] See Appendix B for additional information.

Further, fully effective AV monitoring requires automating reporting, data collection, correlation with other sources.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Continue to use approved AV software on STIP-enabled devices	• Install and enforce the use of anti-virus clients on all TSE • Automate AV definition updates	• Automate AV reporting and data collection • Automate correlation with other data streams and sources (e.g., system logs, compliance scanning, vulnerability scanning)

6.2.3 Activity: Physical Security of Space and Contract Requirements

Description and Benefit: TSA is challenged to establish and enforce physical security standards because the physical layout and operational environment for each airport varies, and TSE reside in non-TSA owned facilities. Deployed TSE can be located in highly trafficked locations that are visible—and, at times, accessible—to the public. OSC collected best practices and developed standard design guidelines, the PGDS the CDG, for airport operators to follow; however, these documents do not place requirements on airport operators nor are they regulatory in nature.

Contractually, OSC collaborates with industry to create and implement physical security requirements throughout the lifecycle of TSE, from initial deployment to retirement. This requires the physical security of TSE to be audited throughout its lifecycle to drive SOP implementation.

Activity Subtasks: OSC must update the PGDS and CDG to reflect additional physical standards for cybersecurity, including prioritizing unprotected network ports for which there are no physical access controls. It is important that OSC address issues related to cable hygiene and labeling. Finally, updated physical design requirements for TSE (e.g., caged network ports) need to be developed and inserted into future procurements to enhance TSE physical security posture. (Goal 1 addresses ways to monitor and enforce physical security.)

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
Security of Physical Space		
Update design guides for: • Locking cabinets; • Restricting physical access to TSE; and • Port security	• Coordinate physical and logical security access control data events to derive insights	• N/A
Physical Security Contract Requirements		
Update guidance/SOPs for: • Data storage devices (e.g., thumb drives); and • Contract language	• Create requirements to enable high maturity access control programs (e.g., Personal Identity Verification [PIV], biometrics)	• N/A

6.2.4 Activity: Logical Security (Software-Based Access Control, Elevated Privileges)

Description and Benefit: Given the recent cyber breaches, logical security has become a priority for DHS. Logical security measures include general safeguards to protect a network and are the first line of defense for OSC's technology platforms. Examples of these measures include requiring strong user names and passwords, filtering traffic, and disabling ports and protocols for network-based access. Thousands of TSOs and TSE end users operate or access TSE on a daily basis. While unauthorized access is typically associated with malicious activity, an authorized user may provide improper user access, or improperly use TSE otherwise (e.g., unapproved thumb drives). Additionally, this risk is heightened as remote access to TSE is enabled by STIP.

Activity Subtasks: The first step of effectively implementing logical security measures is to audit existing users to validate that users are provided the appropriate access levels based on their role and

responsibility, and continue to periodically audit the user pool. To achieve full PIV card implementation and eventual biometric authentication, OSC needs to simultaneously plan for PIV implementation for new TSE, as well as explore options to retroactively apply PIV technologies to existing TSE.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Audit existing privileged users • Coordinate with OSO and airports to encode access user levels in new and existing SOPs	• Broaden adoption of TSE User Management application • Conduct annual Privileged Account Audits • Require vendors to make TSE compatible with TSA-issued PIV cards • Utilize a modified means of applying PIV to legacy technologies while waiting for actual implementation	• Launch PIV implementation • Launch biometric authentication

6.2.5 Activity: Data Encryption and System Interconnection Standards

Description and Benefit: This activity protects data-at-rest and data-in-motion via approved encryption methods and ensures that restricted data cannot be accessed by unauthorized devices. Currently, OSC engages OIT IAD to secure data.

Activity Subtasks: The enhancement of risk-based security may require changes to existing architecture and data flows and the introduction of interfaces to external non-TSANet entities. Interfaces and system demands evolve to meet RBS and security effectiveness requirements, challenging both equipment manufacturers and TSA. Additionally, the introduction of varying levels of secured data in aviation security systems necessitate different encryption levels for data-at-rest and data-in-motion (e.g., personally identifiable information or classified data). Eventually, these activities support use of PKI capabilities for TSE.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Assess external interfaces from a cybersecurity perspective and potentially execute Interconnection Security Agreements between baggage handling systems (BHS) and airport systems • Provide guidance on encryption for communication with external interfaces like BHS • Determine encryption for data-at-rest	• Utilize current IPS-approved Transport Layer Security (TLS) • Require vendors to equip TSE with Public Key Infrastructure (PKI) capabilities • Prioritize the data that should be moved to PKI (rather than TLS)	• Begin use of PKI

6.3 Goal 3: Acquire, Develop, and Test Technologies that Lower Cybersecurity Risk

This goal acknowledges the importance of, and efficiencies gained, by introducing cybersecurity considerations into the early stages of the acquisition lifecycle. It also acknowledges OSC's innate dependence on these third parties to deliver capabilities necessary for mission execution. In order to deploy capabilities in an efficient manner, collaboration early in the development process is critical so that vendors may adjust investments and resources towards meeting cybersecurity requirements.

Goal 3 Framework Elements Applied:
- SELC Integration
- Integration with Other Operations and Incident Response

While Goals 1 and 2 discuss the programs that are necessary to identify and mitigate vulnerabilities, Goal 3 captures activities and subtasks relevant to the acquisition lifecycle that are necessary to secure capabilities. It focuses on the contract requirements and also determines the adequate structure for the testing of cybersecurity requirements.

6.3.1 Activity: Vendor Requirements

Description and Benefit: Partnership with industry is critical in creating sound cybersecurity requirements that protect TSE from cyberattack. OSC works heavily with vendors throughout the acquisition process to communicate its cybersecurity needs and comply with cybersecurity-related requirements.

Activity Subtasks: Since June 2015, OSC has taken steps to enhance vendor compliance with cybersecurity requirements. For example, in July 2015, OSC released nine key cybersecurity requirements for vendors: (1) AV software and definition updates; (2) OS security patching; (3) hardening; (4) technical obsolescence; (5) security scanning support; (6) POA&M support; (7) vendor information system security official (ISSO) designation; (8) PIV compatibility; and (9) SOC monitoring and reporting. Together, these requirements holistically address threats and mitigation tactics throughout the SELC and help OSC comply with federal guidance.

DHS recently mandated that all unsupported operating systems (e.g., Windows 2003, Windows XP) be retired immediately due to the potential for associated security vulnerabilities. OSC has taken significant steps to comply with this requirement, and continues to work with vendors to immediately remediate TSE with expired operating systems that cannot be entirely removed from the screening process (due to their criticality to mission effectiveness). Upon completion of the subtasks, OSC will be better positioned to effectively incorporate cybersecurity into contract language.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Publish requirements to vendors • Retire expired operating systems. • Analyze results of IT security gap analyses from each vendor and determine way forward	• Collaborate with industry to shape future requirements and capabilities	• Implement and control cybersecurity contractual requirements

6.3.2 Activity: Test Infrastructure and Processes

Description and Benefit: Cyber testing involves verifying that vendors have successfully implemented OSC-required cybersecurity measures into TSE, and that these cybersecurity measures do not interfere with the TSE's mission detection capabilities.

Activity Subtasks: To date, scans for operating system hardening are conducted at the TSIF in collaboration with OIT IAD; however, no capability for enhanced cybersecurity testing currently exists. There is no facility that can accommodate testing for both functions, although creation of such a facility is possible with proper budget and resource allocations.

OSC is contracted with JHU Advanced Physics Laboratory (APL) to prepare and executive a test plan and procedures, identify key findings, and provide recommendations for short-term mitigation efforts. Upon receipt, OSC will incorporate appropriate recommendations to finalize its test infrastructure.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Conduct cybersecurity-focused security testing as part of STIP operational test and evaluation activities (e.g., through JHU APL)	• Integrate JHU APL findings, as necessary	• Finalize test infrastructure

6.3.3 Activity: Supply Chain Risk Management

Description and Benefit: Supply chain risk management (SCRM) is the process by which stakeholders maintain the integrity of each component of the supply chain. In response to a requirement of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, the Department of Defense and the General Services Administration jointly issued a report on incorporating security standards into acquisition planning and contract administration, including those for cybersecurity.[9] The report specifically recommends that government agencies issuing acquisitions require contractors to purchase materials from original equipment or component manufacturers, their authorized resellers, or other trusted sources whenever available, and to reference the Qualified Bidders List when selecting providers.

Activity Subtasks: In the future, OSC and OA will work with vendors and other government entities, like DHS' National Protection and Programs Directorate (NPPD), to prioritize supply chain integrity and certify that the products used in TSE have not been compromised prior to integration into TSE. Working with OA, OSC must follow all mandated SCRM practices and, where applicable, insert the appropriate language into contracts to require those practices of their vendors.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Require vendors to provide analysis of suppliers' risk score based on integrity of supply chain	• Develop list/standards for allowed vendors (with DHS NPPD)	• Develop and implement real-time capabilities for determining the integrity of supply chain and individual procurement targets

6.3.4 Activity: Operational Cyber Testing

Description and Benefit: Operational cyber testing is an alternative testing method designed to mirror real-world attacks executed by third parties with no previous relationship to the organization. For example, an organization may employ a cybersecurity red team to conduct external penetration testing. In addition to enhanced network security, these activities may help OSC also address and prepare for external audits.

Activity Subtasks: Operational cyber testing can only be implemented in a highly robust cybersecurity regime. As such, this is only a high maturity task that OSC can conduct after other cybersecurity risk management and network protection measures are achieved.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• N/A	• N/A	• Put cyber red teams in place and conduct routine testing

[9] Department of Defense and General Services Administration. *Improving Cybersecurity and Resilience through Acquisition*. November 2013. http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf

6.4 Goal 4: Assign and Enforce Responsibility to Comply With Policy and Standards

This goal helps OSC understand the resources, organizational considerations, and workforce needs to execute and integrate activities in Goals 1-3. Without the resources and processes in place, the outlined cybersecurity measures are not achievable. Implementing this goal requires OSC to analyze its current workforce and engage in workforce planning efforts to implement the new cybersecurity requirements. It also requires OSC to evaluate and update current processes and organizational constructs so that those processes and organizations effectively address cybersecurity in the short-term and create a basis for ongoing compliance and protection. Overall, Goal 4 is created to address the organizational and workforce implications involved in implementing all other goals.

Goal 4 Framework Elements Applied:

- Transition Planning
- Process Change Management
- Governance
- Workforce Alignment
- Integration with Other Operations and Incident Response

6.4.1 Activity: Workforce Alignment

Description and Benefit: Workforce alignment addresses how OSC staff roles change to accommodate new cybersecurity measures, as well as what gaps may exist in current resourcing and workforce capabilities. Currently, the responsibility for TSE cybersecurity lies with an Information System Security Officer (ISSO).

Activity Subtasks: As a result of federal Cybersecurity Sprint activities, OMB, the Office of Personnel Management (OPM), and DHS are drafting guidance and tools necessary to develop the required blend of technical, policy, and leadership resources needed to cover the multiple disciplines within use hiring and staffing recommendations to augment its existing cyber capabilities to implement current and future cybersecurity requirements. Since responsibility to execute against responsibilities also falls across OSC partners, OSC must coordinate these activities with them.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Establish a clear set of workforce competency requirements based on cybersecurity support needs identified in this plan • Conduct preliminary workforce gap analyses	• Determine OSC/OIT resourcing based on gap analyses • Establish a strong and supported ISSO program within the organization • Establish an internal ISSO support model • Reposition current staff or redefine responsibilities where appropriate • Outline cybersecurity roles and responsibilities	• Establish contracts for engineering support to enable patching • Assess and determine modifications to organizational offices and substructures • Hire additional personnel to address needs

6.4.2 Activity: Training and Change Management

Description and Benefit: Training and change management includes providing training, tools, and other development opportunities to OSC staff and partners to support changing roles or responsibilities in cybersecurity and enable adoption of new security rules.

Activity Subtasks: To achieve the desired end state, OSC must provide discrete training and on the job performance support, including executive briefings, job aids, formal workshops, and one-on-one support sessions. Communications must underscore the importance and impact of cybersecurity actions and reinforce key messages to identified stakeholders.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Determine workforce-wide and mission critical learning needs for OSC (e.g., contract requirements technical training for acquisitions-related roles and engineers), OA, and OIT employees • Prioritize learner groups and topics	• Decide appropriate training or communication vehicle for each stakeholder and message • Design, develop, and implement trainings for partners	• Evolve trainings into scenario- and simulation-based learning to drive improvements in productivity and workforce effectiveness

6.4.3 Activity: Governance

Description and Benefit: Cybersecurity policies and procedures are required to support and manage IT system development and operations according to OSC guidelines. Governance refers to the policies that assign responsibility and authority for cybersecurity actions. Effective governance introduces accountability for individuals and divisions involved in TSE cybersecurity process and delineates clear hand-offs and decision-making processes.

Activity Subtasks: While determining internal cybersecurity responsibilities is a significant activity, OSC leadership must further consider how OIT, OA, and OSO will contribute to or support OSC's cybersecurity goals. Additionally, there is currently overlap in the Change Control Boards (CCB) and engineering design reviews, supported by OSC and OIT. For the CCBs specifically, OSC must work with OIT to first streamline and delineate roles of authority for the CCBs and implement metrics by which is gauge success.

Low Maturity Subtasks	Medium Maturity Subtasks	High Maturity Subtasks
• Map out current and future process for major decisions related to cybersecurity with partners • Crosswalk OIT and OSC governance processes, to include engineering design reviews and the CCB process	• Establish roles and responsibilities for cybersecurity decisions • Define role and structure of integrated governance • Conduct architectural design reviews • Update enterprise architecture processes principles	• Implement and monitor effectiveness of existing roles and processes

7 Plan Execution

Framework Element Applied:
- Transition Planning

There are multiple elements to OSC's cybersecurity plan; addressing all of them simultaneously requires a significant influx of resources (i.e., both staff and funding). Without a full understanding of these resources, OSC cannot yet address ownership or schedules in support the activities listed under of each goal; rather, the plan outlines all the activities that would support a robust cyber risk management capability.

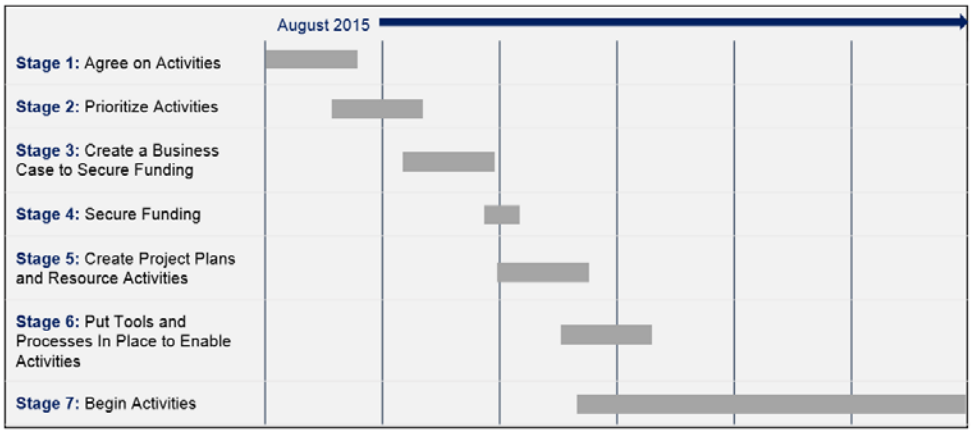
As OSC looks to implement the plan, the next step is to prioritize all outlined activities, determine preliminary resource needs, and build out a high-level roadmap with major milestones, planned resources, and timing to guide the enterprise. Of all the activities and subtasks that underpin the plan, the following five items must be prioritized to secure TSE and its enabling technologies, as well as ensure that OSC is operating within the bounds of regulations set forth by the federal government:

- **Asset Inventory:** Underpins the transition to a mature cybersecurity capability, including asset prioritization, discovery scanning, operating system patching, antivirus updates, and locating and updating obsolete and unsupported operating systems.
- **Basic Discovery Scanning:** Related to asset inventory, enables OSC to confirm its existing inventory and is required for the *Federal Information Security Management Act* and continuous diagnostic and mitigation compliance.
- **Asset Prioritization:** Helps OSC determine how to apply cybersecurity resources to safeguard its most important data and systems, while simultaneously meeting requirements of the government's Cyber Sprint and creating long-term resource optimization.
- **Design Standards for Imminent Procurements to Support Recapitalization:** Helps vendors plan for new TSE cybersecurity requirements.
- **Full Lifecycle Planning:** Completes transition planning for the remainder of the plan implementation over the next several years, including assigning resources and organizational responsibilities for plan implementation.

These five elements also support three of OSC's most critical ongoing cybersecurity efforts: replacing unsupported OS, patching systems, and installing updated AV software on connected TSE.

The implementation of the plan can be accelerated through an extended facilitated leadership working session that spans the leadership teams of OSC, OA, OIT, and potentially other TSA offices. This session would be used to immediately identify a series of next steps that are mutually agreed upon and supported across the offices, as well used to collect info and determine agreements to lay out the longer term roadmap for all goals and activities outlined in this plan. Figure 3 depicts the process OSC follows to initiate the plan.

Figure 3: Programmatic Efforts



8 Conclusion

An increasingly interconnected checkpoint propels TSA into a more dynamic, data-driven state; however, the increased connectivity also comes with the increased risk for cyberattacks. OSC is mobilizing to protect itself against internal and external threats that could have a detrimental impact on mission execution. This plan, and corresponding OSC Cybersecurity Management Framework, equip OSC with the strategies, policies, and tools necessary to achieve a desired outcome where TSE are proactively protected against cyberattack. OSC achieves these partnerships through the execution of goals, activities, and subtasks in this plan, and by internal cross-collaboration with DHS and government agencies, including external cross-collaboration with industry partners.

APPENDIX A: OSC Cybersecurity Management Framework

The nine-element OSC Cybersecurity Management Framework allows OSC to prioritize TSE assets and apply risk-based approaches to secure and maintain mission-critical functions. Elements of the framework were selected and tailored from the foundational policy and compliance documents from NIST, DHS, TSA, and others to craft a framework that accounts for OSC's current environment as well as the OSC vendor community. The framework incorporates nine elements that help OSC implement a robust risk management capability, from transition planning to applying lessons learned for operational improvement. These elements:

- Holistically encompass processes and procedures that identify and manage cybersecurity risks across technical, operational and policy fields;
- Drive OSC's understanding of which assets present the greatest risks based on threats and vulnerabilities and drive resolution and remediation efforts across those assets; and
- Build in considerations for project planning and metrics development and assessment by which to gauge implementation progress.

Figure 4 lists the nine framework elements.

Figure 4: OSC Cybersecurity Management Framework

APPENDIX B: Foundational and Compliance Documents

TSA and other federal departments and agencies have issued policy and compliance documents to help agencies secure their organizations and capabilities from cyberattack. These documents were analyzed and used to inform both the OSC Cybersecurity Plan and Framework. Table 1 shows the OSC Cybersecurity Plan's foundational compliance documents.

Table 1: Foundational Compliance Documents Influencing the OSC Cybersecurity Plan

Outputs of Cybersecurity Management Plan	Foundational Policy and Compliance Documents	Description of Reference Document
FISMA Compliance	NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*	Outlines the general elements of a risk management process
	NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*	Provides guidelines to organizations when security controls to safeguard their networks as part of a risk-based approach to cybersecurity
	DHS 4300A, *Sensitive Systems Policy Directive*	Outlines specific guidance for DHS components to help implement NIST SP 800-37 on unclassified systems, including TSE
	NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*	Helps organizations develop continuous monitoring solutions
	TSA 1400.3, Management Directive *Information Technology Security and Information Assurance Handbook.*	Explains policies and procedures to support the secure use, development, and maintenance of TSA IT systems in accordance with the aforementioned documents
	NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*	Provides recommendations for improving an organization's malware incident prevention measures
Real-Time Data Collection	Office of Management and Budget (OMB) 14-03	Provides guidance for managing information security risk on a continuous basis
Risk Assessment	Carnegie Melon's OCTAVE Methodology	Analyzes an organization's cyber risk. Factors mission and organizational priorities into the asset prioritization process

Additional documents and policy referenced throughout the plan's development are listed below:

- Department of Defense and General Services Administration. Improving Cybersecurity and Resilience through Acquisition. November 2013. http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf
- Department of Homeland Security. *2014 Quadrennial Homeland Security Review.* June 2014. http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf
- Deyo, Russell. Memorandum from the DHS Under Secretary for Management: *DHS Strengthening DHS Cyber Defenses*, July 2015.

- Office of Management and Budget. *DRAFT Cybersecurity Sprint Strategy and Implementation Plan for the Federal Civilian Government.* Release date to be determined.
- Office of Security Capabilities. *Information Assurance Requirements for TSA Government Acquisitions for OSC*. July 2015.
- Transportation Security Administration. *Feasibility of Inventory Tracking Report to Congress*, April 2015.
- Transportation Security Administration. *Enterprise Risk Management Policy Manual*. August 2014.
- Transportation Security Administration. *Strategic Five-Year Technology Investment Plan*. May 2014.
- Transportation Security Administration. *Acquisition Reform Act of 2014 Implementation Strategy*. May 2015.

APPENDIX C: Methodology Used to Determine OSC's Future State

In order to determine the goals and activities that encompass the Cybersecurity Plan, OSC reviewed its strategic goals from a variety of planning documents, discussions from a meeting between OSC and OIT in April 2015, as well as stakeholder feedback from across OSC and its partnering organizations.

1. OSC Strategy and Policy

Specific strategy and planning documents reviewed include:

- Strategic Five-Year Technology Investment Plan (July 2015)
- OSC Strategic Capability Investment Plan (May 2014)
- Information Assurance Requirements for TSA Government Acquisitions (July 2015)

2. OSC/OIT Meeting Collaboration

The OSC/OIT meeting in April 2015 was held to discuss cross-organizational cybersecurity challenges, technological and organizational goals, and activities for OSC/OIT collaboration moving forward. Discussion topics are outlined in Table 2:

Table 2: Technical and Organizational Goals

Goal	
Technology	
TSE Connectivity	• Establish security and organizational boundaries. • Articulate benefits of connectivity.
IT Security Requirements Prioritization	• Create a risk-based framework that can be used to assess IT security requirements and differentiate among assets. • Balance IT security with mission security as it related to cost, schedule, and risk. • Include the ability to measure the success against execution of the plan.
System Architecture	• Consider IT security as a main consideration when conducting system architecture planning efforts. • Create a framework that is flexible enough to apply to future state system architecture principles.
Organizational	
Governance	• List governance elements and owners. • Define roles and responsibilities of owners. • Detail a proposed future state governance structure that accounts for organizational and process change structures.
Workforce	• Define roles and responsibilities of existing resources, including federal information system security officers (ISSO) and contractors. • Articulate gaps in level of effort/skills of existing resources. • Establish a plan for training and workforce development to help stakeholders understand both cyber threats and IT security requirements. • Recommend the inclusion of cybersecurity testing elements in the Test and Evaluation Support Services contract re-compete.
OSC/OIT Collaboration	• Detail a workforce plan for how OSC and OIT collaborate to solve challenges. (e.g., how do OSC ISSOs interact with OIT Information Assurance and Cybersecurity Division engineers?) • Consider the developmental and operational aspects of IT security testing. • Work with OIT to determine the cost of implementation of IT security requirements and protocols and use this document for FY16 spend planning.

Collaboration with Vendors	• Foster industry engagement in the IT security requirements definition process via stakeholder meetings to share and validate requirements. • Consider how to engage industry on IT security requirements via ongoing system architecture planning efforts and changes. • Enable adoption of IT security requirements by establishing hard guidelines with vendors and acknowledging requirements as strict protocol.
Physical Security	• Incorporate compliance with existing design guides (Planning Guidelines and Design Standards, Checkpoint Design Guide). • Assess existing standard operating procedures (SOP) for cybersecurity-related elements and work with OSO on SOP enforcement.

3. Stakeholder Feedback

In order to gather primary source feedback regarding IT security's current and future state, it was necessary to conduct stakeholder interviews. Before beginning interviews, OSC developed a set of questions to collect interviewee's existing attitudes towards IT security as well as highlight any previously unforeseen gaps or implementation challenges around topics such as business drivers, governance, automation, resources, and industry engagement.

During this interview process, OSC had the opportunity to listen to diverse perspectives from all seven OSC division directors and 15 other staff across OSC, OIT, OA, and OSO. After completing all of the interviews, OSC condensed and compiled the responses, allowed for key themes to be effectively extracted, and used in identifying the current and future state of cybersecurity. Major themes that were derived are located in Table 3:

Table 3: Themes from Stakeholder Interviews

Areas	Themes
Governance	• Over 85% of participants believe that the roles and responsibility related to IT security are NOT well defined within their respective stakeholder group. • Some participants believe that although some form of a change management process exists it does NOT currently address IT security related changes.
Workforce	• Over 90% of participants believe the resource capabilities are NOT sufficient to support an IT security plan implementation. The most common solutions to insufficient resources were bringing in external IT security experts to help with subtasks such as requirements and testing and utilizing resources from OIT. • Over 90% of participants believe that additional trainings or discussions are necessary to explain the purpose of the IT security plan and how it affects stakeholders and their respective organizations.
OSC/OIT Collaboration	• Over 70% of participants believe there needs to be increased collaboration between OIT and OSC in order for both groups to have a better understanding of how each other function, their roles and responsibilities, and the mission.
Collaboration with Vendors	• A majority of participants believe there needs to be more frequent and substantial interactions with industry in order to effectively communicate requirements and solicit feedback, better involve the industry's experts, and better educate the importance of increased IT security and the severity of cybersecurity threats.
Physical Security	• There was general disagreement on whether existing design guides are followed, but participants expressed a need for increasing the guide's coverage over physical security of TSE and more effective methods for continuous monitoring to maintain compliance.

Other	• Over 80% of participants believe a successful implementation approach would either be a top-down method in which leadership develops a strategy or a hybrid method in which leadership develops the requirements and direction utilizing the engineering expertise regarding implementation feasibility. • A majority of participants believe that leadership has made IT security a priority focus. • A majority of participants believe that the current level of cybersecurity risk management automation is minimal, but that automation is a positive endeavor. • A majority of participants foresee challenges to implementing an IT security plan throughout the entire Systems Engineering Lifecycle for a range of reasons including resource and budgetary constraints, constant change in cybersecurity requirements, etc. • Generally, participants understood the benefits of an IT security plan, but stressed the importance of effective communication across the organization to assure support and an understanding over responsibilities.

APPENDIX D: Stakeholder Interview Questionnaire

The following questionnaire was used to survey 22 stakeholders across OSC, OIT, and OA stakeholders in an effort to solicit feedback on the current and future state for OSC cybersecurity in addition to any challenges and/or gaps. The feedback was analyzed to produce themes and incorporated into the plan's goals, activities, and subtasks.

1) **Overview**
   a) What does IT security and cybersecurity risk management mean to you?
   b) Describe how you see an IT security framework and plan for TSE benefitting your office and OSC?
   c) What is senior leadership's position on IT security?
   d) Do you feel that the organizational structure within OSC supports effective cybersecurity risk management? Why or why not?
   e) Let's say that TSE were under a cyberattack. Describe your perception of a worst-case scenario.

2) **Business Drivers**
   a) How will a successful IT security strategy improve what you do on a day-to-day basis?
   b) Describe the existing connection between IT security and mission effectiveness. Is your perception accepted across the organization?
   c) Do you think that existing IT security practices within OSC are focused on checking the box (compliance) or driving business and process efficiencies?

3) **Implementation**
   a) Which of the following options do you think would be a more successful approach to rollout an IT security plan and why?
      i) A bottom-up approach developed by engineers that is then rolled up to the enterprise level
      -OR-
      ii) A top-down, or enterprise, approach that implements a series of policies and procedures and requires the implementation of these procedures by all levels of the organization
   b) Do you see any challenges to implementing an IT security plan throughout the entire Systems Engineering Lifecycle (SELC)?
   c) How will we know when this IT security plan has been successful? What is the desired end state?
   d) In your opinion, what is the most important element to a successful enterprise implementation of IT security strategy?

4) **Governance**
   a) To what extent do you think roles and responsibilities related to IT security are clearly defined in OSC? In TSA as a whole? If they are not clearly defined, what could be done to provide clarity?
   b) How do you think OSC and OIT can collaborate to solve challenges related to IT security? Are there currently barriers to the type of collaboration needed and, if so, what are they?
   c) Does your organization have an established process for managing changes to TSE? If so, how does this process work with IT security-related changes?
   d) Do you think a more robust level of governance and configuration management is needed?

5) **Automation**
   a) What is OSC's current level of cybersecurity risk management automation (e.g., vulnerability scanning; automated approval workflows; extract, transform and load procedures for data warehousing)?
   b) What is your opinion around increasing automation of cybersecurity risk management within OSC?

6) Resources

a) Do you think current resource capabilities within OSC are sufficient to support an IT security plan implementation? If not, where should these resources come from (e.g., external hire, detailee)?

b) After a plan is established, is there additional training that you think should occur to educate employees on how to implement the plan? If so, describe what these would look like.

c) Do you feel that individuals within your office are interested in IT security and would be willing to modify their current job roles or take on additional responsibilities to support implementation?

7) Industry

a) How can OSC better collaborate with industry to improve compliance with IT security requirements in future system design efforts?

   i) What types of incentives would compel industry to adopt OSC's IT security requirements?

8) Physical Security

a) In your opinion, to what extent do OSC stakeholders follow existing design guides (e.g., Planning Guidelines and Design Standards, Checkpoint Design Guide) and are those guides effective to help secure TSE from threats in their physical environments?

b) Describe existing access control standards and their effectiveness in subduing an insider threat within TSA.

9) Additional Concerns

a) Of all of the issues discussed today, which two are the most important to creating a successful plan that will increase the cybersecurity of TSE?

b) Do you have any other concerns or inputs that we should consider when developing the draft plan?