Transportation Security Administration

Office of Security Capabilities
Cybersecurity Management Framework

Version 1.5

Updated: August 10, 2015

The contents of this framework 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. This framework is not intended to supersede any existing compliance related policy enforced by the TSA Office of Information Technology. Additionally, this framework is flexible to adapt to changing requirements, guidance, policies, and procedures.

Table of Contents

1 Introduction

Federal agencies face a dynamic cyber threat environment against highly-skilled adversaries capable of mounting crippling attacks on our nation's critical infrastructure. The threats range from foreign actors stealing classified data to terrorist groups launching attacks on systems that protect and serve our nation, which include transportation screening equipment (TSE) and enabling technologies. These technologies help manage the risks linked to explosive detection and other malicious threats to the nation's transportation systems. In addition to malicious actors, TSE operator error may also introduce vulnerabilities to TSE, such as inserting unencrypted or infected thumb drives into TSE. Leaving TSE and enabling technologies vulnerable to these types of security incidents diminishes the assets' ability to detect threats, potentially allowing a malicious actor to smuggle an explosive or other substance through the checkpoint, which could cause infrastructure damage or even potential loss of life.

OSC Mission

OSC implements advanced security solutions to protect the Nation's transportation systems, ensuring freedom of movement for people and commerce. Critical to achieving OSC's mission is the ability to adapt its processes and capabilities to address dynamic, evolving threats posed to the nation's transportation network. As such, OSC collaborates with industry and transportation stakeholders to build, test, field, and sustain the breadth of TSA's security capabilities and field operations. OSC also engages with international partners to harmonize technology operating standards, which enhances global transportation security.

Given the current cyber threat environment, the Office of Security Capabilities (OSC) must anticipate that adversaries will attempt to exploit TSE vulnerabilities. OSC faces significant challenges in securing both networked and non-networked TSE and related assets. Mitigating these challenges is increasingly difficult due to the complexity of OSC's mission and dispersed operating environment; OSC has deployed over 15,000 TSE with over 250 operating configurations and 50 security configurations across 450 federalized airports. Given fiscal realities and the evolving threat landscape, it is critical to dynamically prioritize risk mitigation, focusing on the highest risk areas first. Building on the compliance assessment efforts already in place to inform risk-based decision making optimizes resource allocation and improves the effectiveness and efficiency of securing and maintaining a heightened security posture for the aviation systems and continued industry growth. This allows OSC to continue to support the ever-growing transportation industry, while protecting the equipment and capabilities that support the OSC mission from emerging and dynamic cyber threats.

This document outlines a cybersecurity management framework and risk-based approach to securing and maintaining OSC's mission-essential functions. This framework:

- Describes the benefits of a risk-based management approach;
- Provides detailed information on each of the framework's nine elements; and
- Explains how OSC stakeholders implement and use the framework.

OSC will apply this framework when developing the OSC Cybersecurity Plan. The plan will include the goals, activities, and low- , mid-, and high-maturity subtasks necessary to execute the framework elements outlined herein. Adopting this approach to manage the security challenges and risks to the mission helps OSC achieve a flexible and adaptable cybersecurity risk and decision policy that will best position it to identify, protect against, respond, and recover from cybersecurity threats. This framework supports the overarching Risk Management Framework required of Department of Homeland Security (DHS) components by enabling TSE to reach the maturity level to be compliant therein.

2 Objectives of the OSC Cybersecurity Management Framework

OSC's 2014 Security Capability Investment Plan discusses the Transportation Security Administration's (TSA) commitment to pursuing risk-based security, noting that TSA "must take further steps to integrate diverse data sources in near real-time and develop the analytical, technical, process, and human capital assets needed to operate a complex and dynamic system."[1] Moving cybersecurity into a risk-based

[1] OSC. *Transportation Security Strategic Capability Investment Plan*. May 2014.

model not only aligns to TSA's strategic goals, but also drives mission effectiveness by improving the integrity of OSC assets. It also creates long-term resource optimizations and cost avoidances; and positioning OSC to comply with the DHS Risk Management Framework and respond to the future cyber threat environment and government requirements.

2.1 Increasing Mission Effectiveness

OSC's Cybersecurity Management Framework:

- Identifies the mission-critical assets and systems that require continuous protection;
- Facilitates conversations among OSC officials around risk trade-offs (i.e., level of risk acceptance or avoidance to OSC assets);
- Prioritizes assets and the necessary resources to protect them, guiding OSC in long-term investment planning to continuously improve the security of all OSC assets; and
- Offers a repeatable and actionable method to approach additional challenges, such as clearly defining the cybersecurity capability requirements for TSE vendors in standard contract language.

2.2 Enabling Long-Term Resource Optimization and Cost Avoidance

OSC's Cybersecurity Management Framework:

- Creates process efficiencies around data collection and other technological solutions to derive risk scores that align with the annual DHS Information Security Performance Plan; and
- Eliminates or minimizes duplicative roles and responsibilities among OSC staff, allowing reallocation of resources for cybersecurity technological solutions.

2.3 Positioning OSC for the Future

OSC's Cybersecurity Management Framework:

- Is flexible and extensible to address today's dynamic cybersecurity environment, while also adaptable to address future unknown threats and emerging vulnerabilities;
- Is adaptable to DHS' dynamic and fluid cybersecurity requirements, such as the 2015 Cyber Sprint and Cyber Defenses requirements;
- Is designed as a series of elements that can be interchanged to achieve different cybersecurity outcomes, allowing the framework to adapt to OSC's evolving mission and threat landscape; and
- Helps OSC proactively comply with the DHS National Protection and Programs Directorate's (NPPD) Continuous Diagnostics and Mitigation (CDM) Program.

3 Foundational Documents

In response to the evolving cybersecurity environment, the Federal Government, including TSA, has issued multiple reference documents and supported initiatives to help agencies implement a cybersecurity management framework. The OSC Cybersecurity Management Framework was built on and aligns to the following documents and methodologies:

- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations;

- DHS 4300A, Sensitive Systems Policy Directive;
- TSA MD 1400.3, Information Technology Security;
- Office of Management and Budget (OMB) Memorandum 14-03, Enhancing the Security of Federal Information and Information Systems; and
- Carnegie Mellon University's Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Methodology

The documents were intentionally selected to provide for process and organizational efficiencies, as well as drive compliance with existing and future laws, such as the *Federal Information Security Modernization Act*, and Executive Branch regulations published by NIST and DHS. This framework is not intended to supersede any existing compliance related policy enforced by the TSA Office of Information Technology. Appendix B contains additional information on how OSC applied each document.

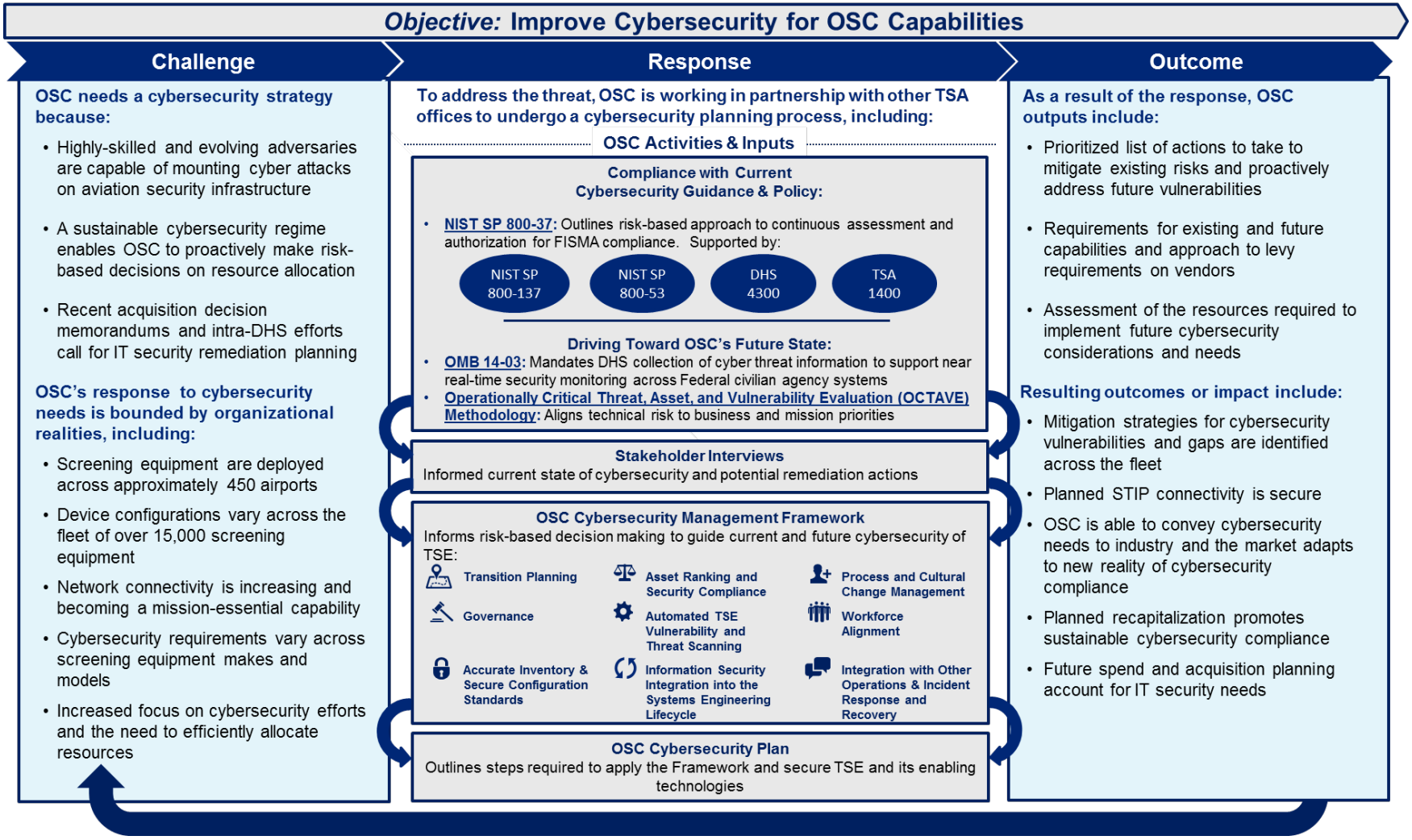
4 Cybersecurity Management Framework

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 documents from NIST, DHS, TSA, and others to craft a framework that accounts for OSC's current environment as well as the TSE 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 1 depicts how the current operational environment, regulatory requirements, and framework elements come together to drive outcomes of the Cybersecurity Management Framework.

Figure 1: Development and Application of the Framework to Drive OSC's Future State



Together, the framework elements enable OSC leadership to make risk-based decisions on cybersecurity for TSE and its enabling technologies. The following subsections discuss the nine framework elements, how OSC implements them, and the outcomes that each realizes for OSC.

4.1 Transition Planning

Defining Transition Planning and Implementation Steps

Transition planning lays the foundation for successful framework implementation. OSC involves key stakeholders (both internal and external) in the planning process to capture important mission priorities and outline the steps needed for a successful Cybersecurity Management Framework implementation. Implementation goals are clearly defined and actionable while making sure involved stakeholders understand their roles and responsibilities before, during, and after the transition. These stakeholders also define metrics to serve as indicators of success and progress throughout the implementation process.

Transition decisions drive implementation schedules and resource allocation, and transition planning further requires OSC leadership to determine schedules around framework implementation and define short, medium, and long-term priorities. Finally, leadership aligns the appropriate resources to effectively implement the framework, including both fiscal and staff support.

A comprehensive transition plan to begin implementing the Cybersecurity Management Framework accounts for OSC's unique characteristics (e.g., integration with Office of Information Technology [OIT] and Office of Security Operations [OSO], dispersed nature of TSE), leverages OSC resources, and aligns to TSA's Enterprise Risk Management Strategy.[2] At a minimum, it encompasses the following activities:

- An assessment of the current environment, (e.g., processes, resources, software, and hardware);
- A decision on which components of the Cybersecurity Management Framework OSC will implement;
- The part of the organization in which OSC will implement the framework elements (e.g., division, branch, or system);
- A timeline for framework deployment; and
- A staffing and resource plan to support framework implementation.

Outcomes

A transition plan establishes short-, mid-, and long-term paths forward and positions OSC to receive buy-in from key internal and external stakeholders on how the Cybersecurity Management Framework impacts existing acquisition and program management. Through transition planning, implementation needs are recognized and addressed across stakeholders external to TSA, and to points of contact responsible for implementing the framework.

4.2 Governance

Defining Governance and Implementation Steps

Governance refers to the policies and procedures (e.g., DHS 4300A, TSA MD 1400.3) that assign responsibility and the organizational constructs (e.g., boards or committees, such as OSC's Configuration Control Boards) that support them for cybersecurity-related actions. Cybersecurity policies and procedures are required to support and manage IT system development and operations according to OSC guidelines. Developing these policies and procedures as part of an overall IT governance model provides an enterprise framework for information security risk management. This holistic approach provides OSC-wide coordination and oversight of IT security operations and initiatives, and promotes operational excellence, which can lead to risk reduction and cost savings.

[2] The ERM includes TSA's Risk Appetite Statement that articulates the level of risk TSA will accept in relation to the anticipated consequence. See: *Transportation Security Administration Enterprise Risk Management ERM Policy Manual*. August 2014

At a minimum, governance policies include clearly defined:

- Responsibilities that are assigned to a specific job title or function;
- Lines of authority so that OSC's cybersecurity practices align to individuals who understand and can make decisions on cybersecurity;
- Methods to ensure that the organization continues to comply with Federal security regulations;
- Performance metrics to communicate goals and outcomes for various tasks; and
- Process improvement and remediation actions.

Governance policies are also extended to vendors, when applicable, via acquisition guidelines.

Outcomes

Effective governance introduces accountability for individuals involved in TSE cybersecurity process and delineates clear hand-offs and decision-making processes to reference as the operating environment evolves.

4.3 Accurate Inventory and Secure Configuration Standards

Defining Accurate Inventory and Secure Configuration Standards and Implementation Steps

Given OSC's goal of near 100% network-connected TSE, the need for an accurate TSE inventory becomes paramount. An accurate inventory count of TSE involves cataloging all systems, resources, hardware, and software and associating them to OSC's operations. Gaps or errors in the inventory can cause significant downstream adverse effects, including errors in reporting, misallocation of resources, or assets left vulnerable to multiple attack vectors.

Similarly, secure configuration standards provide the foundation through which security requirements can be established to facilitate consistent configuration settings for TSE, and to promote alignment with security leading practices. The implementation of these standards improves the security posture of OSC by establishing rules that govern the development, operations, and maintenance of system components. It also provides OSC's stakeholders with an understanding of expected system behavior to better prevent and detect abnormal system activities. Maintaining over 250 configurations currently in place amongst the TSE environment is not only unsustainable, but prevents key security activities, such as automated scanning, from taking place. In addition, OSC personnel are unable to invest appropriate resources across the various configurations, as efforts are spread thinly across the gamut of TSE devices.

To implement this element, OSC first manually verifies its existing inventory. Following that, OSC develops processes to manage how TSE is added or removed and then uses technology enablers to implement ongoing monitoring processes. Concurrently, OSC collaborates with internal and external stakeholders to develop secure configurations for TSE. As there is already extensive work established in these areas, the following Government and industry bodies' security configuration standards are used as the basis for development:[3]

- NIST
  - United States Government Configuration Baseline
- Defense Information Systems Agency (Security Technical Implementation Guides)
- Center for Internet Security

As part of secure configuration development, OSC associates individual requirements to DHS and TSA required controls (e.g., DHS 4300A, TSA MD 1400) and NIST SP 800-53 controls. Additionally, it works with stakeholders to capture and review deviations to secure configurations and establish customized configurations tailored to specific TSE. These custom configurations allow OSC to accommodate specific operational needs and identify compensating controls for deviations while minimizing security risk.

[3] These steps are performed in accordance with National Vulnerability Database guidelines.

Outcomes

An accurate asset inventory is a critical foundational element of the OSC Cybersecurity Management Framework. Not only will it help improve security within the TSE environment by tightly controlling network access verified resources, it will also help to identify potential operational inefficiencies caused by redundancy.

Secure configuration standards can be prescribed for vendors to employ in new TSE procurements, for new IT applications within OSC, and in support of the overall OSC enterprise architecture. As currently deployed TSE reaches end-of-life and OSC mobilizes for recapitalization, it can work to build a secure environment during by acquiring TSE that are developed in compliance with standards and requirements, instead of retroactively applying security layers.

4.4 Asset Ranking and Security Compliance

Defining Asset Ranking and Security Compliance and Implementation Steps

NIST SP 800-37, reflected in DHS 4300A, helped shift security programs to a newer, more effective paradigm where IT assets are differentiated primarily on risk posture. This policy currently drives all compliance activities supported by OIT.

While fully accounting for required security controls, OSC's 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.

The process of risk ranking allows OSC's system owners to make well-informed risk-based decisions on implementing safeguards and prioritizing resource allocation. In addition, it helps bolster compliance with IT security mandates, and encourages risk considerations when handling compliance matters.

To establish a risk ranking, OSC evaluates both the business process factors affecting an asset as well as the technical factors that drive cybersecurity vulnerabilities.

- **Business Process Factors**. These factors relay information about the TSE's role in mission execution. An example of a potential business process factor is the type of screening that the TSE is used for (primary screening versus secondary screening).
- **Technical Factors.** These factors include information about the technical characteristics of the TSE system and the technical impact of risks and vulnerabilities on these systems. Examples of technical factors include logical location on a network and support levels for current TSE operating systems.

OSC creates 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 the TSE. This risk ranking is applied to each of the required security controls in the Risk Assessment document to capture the relative importance of each security countermeasure. Individual Component Risk Profiles enable OSC to make more efficient and effective decisions regarding the allocation of security resources, as well as the implementation of safeguards around a given system. The risk ranking methodology will follow the same weighting algorithm as the Common Vulnerability Scoring System.

Outcomes

The Risk Profiles provide OSC the inputs for a centralized repository of security-related information on the systems within their inventory, including a compliance statement for all required NIST security controls. The risk scores could be depicted via tiered dashboards that prioritize OSC's higher risk areas across various levels (e.g., division, system). This risk data is valuable because it prevents stakeholders from becoming overwhelmed by a large list of issues that require attention and instead motivates them to act

against a prioritized list of the highest risk items. In addition, as remediation cost (as either level of effort, dollars, or both) becomes available, this data is integrated to prioritize cost-effective security fixes to the environment. This complements the CDM dashboard by providing a mission-adjusted priority for remediation.

4.5 Automated TSE Vulnerability and Threat Scanning

Defining Automated TSE Vulnerability and Threat Scanning and Implementation Steps

Full operational maturity will require OSC to transition from reliance on labor-intensive, manual assessment policies to a fully automated capability that supports near real-time data capture. By leveraging existing tools and incorporating new capabilities, OSC creates a best-of-breed automated assessment infrastructure capable of identifying security vulnerabilities and misconfigurations in near real-time. Vulnerability and threat scanning reduces the time and resources necessary to conduct security assessments, making it feasible to perform continuous monitoring of information systems and improve the security posture of OSC. It also helps OSC drive to a future state of a flexible and adaptable risk-based cybersecurity regime while complying with OMB's CDM requirements.

Implementation of this element requires:

- Immediate deployment of periodic scans for STIP-enabled devices;
- Analysis of OSC's technology program; and
- Phased implementation of STIP on all TSE.

Concurrently, OSC aligns the results from scans to risk profiles. This allows results to be aligned to the relative importance of the risk with regard to the mission. As deficiencies are identified, OSC uses asset prioritization to determine which items to mitigate first.

Outcomes
Automating manual processes bolsters accuracy and allows a higher standard of protection due to the removal of human error while realizing process efficiencies. It also allows OSC to cover more equipment in greater detail than it could realize previously. As the number of TSE connected to the network continues to increase, automation provides a sustainable approach to securing assets.

4.6 Information Security Integration into the Systems Engineering Lifecycle

Defining Systems Engineering Lifecycle (SELC) Integration and Implementation Steps

OSC is charged with securing its TSE against various cybersecurity attack vectors and, in many cases, making up for security engineering shortfalls intrinsic to the machines themselves. This reactive approach is limited in its effectiveness and costs the organization more than it would to enable proper security functionality during initial product development. The implementation of an SELC integration program serves as a strategic initiative to improve the long-term sustainability of OSC's efforts to secure TSE and improve operational efficiencies. Understanding the unique security considerations for a system in design allows OSC to make timely, cost-effective decisions about which security features are important to implement and which provide little, if any, cost benefits. It also helps to quantify the outstanding risk and associated business impact from unmitigated vulnerabilities.

Successfully integrating information security into the TSE SELC requires substantial involvement from the Office of Acquisitions (OA). OSC can significantly secure its security posture by pushing equipment vendors to close gaps and implement security during the design phase. Implementing security features in the initial design phases is not only more effective, but is often faster to implement at a lower cost.

OSC's SELC implementation program involves efforts before, during, and after TSE acquisition.

- **Pre-TSE Acquisition.** During this phase, TSA collaborates with vendors to set expectations around security requirements for network-connected TSE. This phase may include prescribing certain approved software packages, configuration baselines, standardized security controls, or physical security measures specific to the device. TSA communicates to vendors that securing

TSE is not optional and non-compliant TSE may be disqualified or down-selected during the acquisition process. TSA also communicates to vendors that security gaps which require mitigation by OSC may be charged against the contract as a reimbursable expense. These communication processes helps incentivize performance early in the process.

- **During TSE Acquisition.** In preparation for TSE procurement, OSC formalizes the efforts during the pre-TSE acquisition collaboration phase. This may include requiring certain policies, such as:
  - Use of most current, compliant TSA platforms and secure configurations;
  - Presence of physical security measures to help prevent tampering;
  - Service-level agreements to address vulnerabilities within a set timeframe (e.g., address high-risk zero-day vulnerabilities within 72 hours); and
  - Consequences of non-compliance (e.g., cost reimbursement for risk mitigation by OSC, contract cancellation).

  In addition, OSC works with OA to ensure that evaluation criteria is appropriately weighted to account for security and with OSC's Testing and Evaluation (T&E) Branch to evaluate technological capabilities to determine any gaps.
- **Post-TSE Acquisition.** The T&E team confirms that the vendor addressed any gaps that OSC identified during the acquisition through user acceptance testing, regression testing, and security assessment testing. OSC then uses the asset prioritization model to determine if security deficiencies are material deficiencies and determine if the issues can be mitigated or are outweighed by other factors.

  After the acquisitions process, OSC uses the same asset prioritization model to mitigate the highest-risk deficiencies first. While the SELC integration process should help to significantly reduce these issues, the model provides a means to further minimize the potential impact to operations.

Outcomes

Through integration of security throughout the SELC process, OSC is positioned to capitalize on several benefits, including:

- **Security established during product development**. With collaboration between OSC and vendors, improved contractual requirements, and checks and balances during testing and evaluation (T&E), TSE arrive on-site with improved security posture and experience reduced deployment times.
- **Reduced number of baselines to secure and manage over time**. As existing machines reach end-of-life and vendors comply with OSC requirements for new TSE, the myriad of platform configurations are reduced. In turn, this reduces operational overhead for vulnerability and compliance scanning.
- **Targeted risk mitigation post-acquisition of TSE**. Using the asset prioritization risk model, OSC prioritizes the resultant T&E deficiencies for mitigation by the vendor or OSC (as appropriate). This enables OSC to consider mission and security risk in accordance with organizational timelines to minimize impact on security operations. To minimize the time OSC is exposed to those vulnerabilities, it addresses the highest-risk items first.
- **Improved physical security of TSE**. As vendors meet OSC's physical security requirements, TSE will come with tamper-resistant measures pre-installed. This minimizes the initial risk to OSC, expedites time to deployment, and reduces both the deployment and maintenance costs over time.

4.7 Process and Cultural Change Management

Defining Process Change Management and Implementation Steps

The successful deployment of the Cybersecurity Management Framework within OSC is heavily predicated on a change management strategy that provides role-based training to help users learn their new roles and responsibilities. Approaching role-based training is understood in the context of an overall change management strategy that identifies changes to the cybersecurity management program, assesses the impact of the changes, and manages these impacts. This strategy results in the acceptance of changes and minimal disruption to business units.

OSC develops and executes a process change management plan that takes into account the unique characteristics of TSE, leverages the capabilities of its existing workforce, and aligns to the Cybersecurity Management Framework to:

- Promote tighter integration between OSC and other components within TSA (e.g., OA, OIT) along with other departments and Federal entities as it incorporates risk management concepts in other cybersecurity operations;
- Develop informational and training materials to provide internal communications on the progress of Cybersecurity Management Framework program initiatives. This may include meetings and briefings with system owners and information systems security officers to communicate the OSC mission, Cybersecurity Management Framework methodologies, and leading practices;
- Develop and deliver presentations and briefs to provide external communications that promote the progress of the OSC Cybersecurity Management Framework; and
- Solicit feedback on the effectiveness of transition efforts and potential process improvements in order to tailor future approaches.

Outcomes
Largely a human capital function, development efforts around process change management helps transition the organization to a Cybersecurity Management Framework. Benefits include reduced resistance from stakeholders and increased understanding of individual roles throughout framework adoption.

4.8 Workforce Alignment

Defining Workforce Alignment and Implementation Steps

Stakeholder management and intra-OSC management is imperative for a successful Cybersecurity Management Framework transition. Development of a comprehensive transition plan that takes into account the unique characteristics of TSE, leverages the capabilities of the existing workforce, and aligns to the overall risk management strategy streamlines the transition process.

Along with transition management, OSC disseminates communications around overall Cybersecurity Management Framework efforts and timelines, how personnel roles will change, and what employees can expect. OSC involves stakeholders in extensive training, including executive briefings, job aids, and one-on-one support sessions. Communications include the value of the Cybersecurity Management Framework and an explanation of why OSC is better positioned, in both the short- and long-term, against TSE cyber risk.

Outcomes

A shift in resources and/or job roles allows TSA the organizational bandwidth to address the mitigation of high risk assets.

4.9 Integration with Other Operations and Incident Response and Recovery

Defining Integrating with Other Operations and Incident Response and Recovery and Implementation Steps

As OSC matures its capabilities within the Cybersecurity Management Framework, integrating with other operations provides OSC an opportunity to expand security of TSE beyond its office. This allows OSC to benefit from other offices across TSA dedicated to other security capabilities (such as vulnerability scanning from OIT) and focus on its mission.

Integration with other operations is an intrinsic part of the Cybersecurity Management Framework. The SELC integration aligns OSC with OA to manage vendor risk and shift the effort of securing TSE to vendors over time. Collaboration with OIT enables OSC to have TSE scanned for vulnerabilities, similar to IT infrastructure, without standing up a dedicated resource-intensive capability in-house.

This framework element also accounts for incident response and security log monitoring via the SOC. Though some aspects are covered by satisfying security controls via asset prioritization (e.g., tabletop exercises), OSC also develops a comprehensive mitigation and triage plan. This mitigation and triage plan includes scenario planning exercises to determine how OSC and TSA would respond and recover from a potential cyber attack.

Similarly, OSC conducts exercises with the Security Operations Center and Network Operation Center to confirm that involved parties are appraised and aware of mitigation procedures ahead of a zero-day incident.

Furthermore, consideration is given to the physical security of TSE. While SELC security integration can significantly improve the physical security of newly procured TSE, OSC formulates plans to: (1) secure existing TSE and (2) bolster physical measures in the vicinity of TSE. As necessary, OSC can collaborate with the TSA's Real Estate office as well as local TSA and Airport Authorities to implement compliant physical security controls.

Outcomes

The integration not only provides OSC with additional insight into its assets, but enables increased collaboration and support. Teaming with incident response enables OSC to highlight opportunities and threats, and identify unintended consequences and unanticipated cyber events. It also allows stakeholders to make more informed choices based on a clear and explicit understanding of risk management strategy and market offerings, and an ability to test strategies and formulate responses.

5 How to Apply the Framework

The Cybersecurity Management Framework guides OSC leadership and stakeholders when conducting cybersecurity planning to achieve prioritized risk-based outcomes (e.g., spend planning and budget discussions, acquisition planning, OSC industry days). In preparation for framework implementation, OSC will assign ownership and accountability (i.e., one individual, division, or portfolio) to maintain and drive implementation. This resource requires:

- The requisite technical background to perform as the subject matter expert in the framework elements and understand how OSC can apply the framework to achieve various outcomes; and
- The authority to update the framework as necessary to account for changes in operations, missions, and the cybersecurity environment.

When OSC adopts the Cybersecurity Management Framework, it formally commences transition planning to determine the specific cybersecurity outcomes that it wants to achieve (aligned with strategic organizational goals or compliance). OSC then undertakes an assessment of the current state of TSE cybersecurity and inventories its current assets. Following those activities, the elements of the framework that OSC implements (and to what degree) are largely based on the gaps in OSC's current operational maturity and organizational goals. For example, to help enhance physical security, a framework user could focus on combining elements of asset prioritization, SELC integration, and integration with other

operations.

OSC's ability to implement and adopt the Cybersecurity Framework depends on collaboration and partnership with multiple stakeholders. Table 1 details these groups as well as areas of collaboration. (See Appendix A for additional partnership information.)

Table 1: OSC Partnerships and Areas of Collaboration

Partner	Role in Cybersecurity Adoption and Interaction with Framework
Industry/Original Equipment Manufacturers/ Other Vendors	• Works with OSC to understand the evolving cybersecurity requirements to design and implement compliant capabilities
TSA Office of Security Operations	• Works with OSC in the areas of access control, insider threats, and physical security, as necessary, to safeguard deployed equipment
TSA Office of Information Technology	• Enacts TSA and DHS cybersecurity policy and works with OSC to apply policy • Serves as subject matter experts to OSC on technical information assurance and cybersecurity requirements • Manages compliance and oversight
TSA Office of Acquisition	• Assists OSC in determining the appropriate acquisition and contracting strategies to implement new requirements • Provides guidance for future industry engagement efforts
DHS Science and Technology Directorate	• Works with industry to shape research and development before and in conjunction to OSC development of requirements.

6 Conclusion

OSC's current operating environment, organizational realities, and cybersecurity threat environment present challenges to securing TSE and its enabling technologies. The Cybersecurity Management Framework's elements factor multiple Federal and departmental guidelines to holistically address cybersecurity risks. By implementing the framework, OSC positions its organization to drive mission effectiveness, create resource and process efficiencies, and position itself for future success.

APPENDIX A: Office of Security Capabilities Partnerships

OSC's ability to implement and adopt cybersecurity measures depends on collaboration and partnership with identified stakeholders. OSC manages the acquisition process for transportation screening equipment (TSE), from solution identification through deployment and operations support; however, it partners with stakeholders for specific acquisition lifecycles and broader ongoing business processes. Within a specific acquisition, the Department of Homeland Security's Science and Technology Directorate (S&T) and Original Equipment Manufacturers (OEM) shape research and development before and in conjunction with OSC's requirements development process. Proactive engagement of DHS S&T and industry is critical to shape options to deliver innovative solutions in a budget and threat-constrained environment and enable implementation of cybersecurity requirements. Following the execution of a procurement and resulting delivery of the technology capability to the field, the Office of Security Operations (OSO) is the technology's end user. Partnering with OSO is critical to identify feasible technology and procedural solutions and influence their adoption over time.

Throughout the lifecycle of a mixed-life acquisition program, OSC partners with the Office of Acquisitions (OA) to engage industry vendors and execute purchases. OA plays a critical role in translating requirements to vendors and identifying acquisition strategies to enable application of requirements. OSC partners with the Office of Information Technology (OIT) to achieve compliance with information technology requirements. OIT informs integration of cybersecurity requirements.

APPENDIX B: Foundational Documents

The Federal Government, including the Transportation Security Administration (TSA), has issued multiple reference documents and supported initiatives to help agencies implement a cybersecurity management framework, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The Cybersecurity Management Framework leverages the documents and methodologies outlined throughout this section while also aligning to existing Department of Homeland Security (DHS) and TSA IT security and risk management policies. The documents were intentionally selected to drive compliance with existing *Federal Information Security Management Act* (FISMA), NIST and DHS regulations, while also providing for process and organizational efficiencies. Table 2 shows the primary source documents as well as their strength of influence in the framework's development.

Table 2: Foundational Documents Influencing the Cybersecurity Management Framework

Outputs of Cybersecurity Management Framework		Foundational and Supporting Documents	Strength of Influence*
FISMA Compliance	Risk-based approach to continuous assessment and authorization	• NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* • NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations* • DHS 4300A, *Sensitive Systems Policy Directive* • NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* • TSA MD 1400.3, and *Information Assurance Handbook*	3
Real-Time Data Collection	Collection and consolidation of real time security statuses of IT assets; prioritized asset and vulnerability list	Office of Management and Budget (OMB) Memorandum 14-03	3
Risk Assessment	Aligning technical risk to business and mission priorities	OCTAVE Methodology	1

**3 being most important, 1 being least important*

B.1 Compliance with Federal Policies

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, outlines a six-step process for risk management for Federal IT systems and serves as the basis of the Cybersecurity Management Framework.[4] The process was designed to replace the previous three-year certification and accreditation cycle and move toward a dynamic risk management model. Specifically, NIST SP 800-37's Risk Management Framework enables and supports:

- The implementation of technical, operational, and management controls to enhance information security across Federal IT systems;
- Real-time monitoring and visibility into the security of an agency's network, with the ability to support predictive risk analysis;
- Information sharing for senior agency leaders on which to base decisions around the agency's acceptable risk posture related to its IT systems;

[4] NIST. SP 800-37. *Guide for Applying the Risk Management Framework to Federal Information Systems* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

- Incorporation of cybersecurity measures into the system architecture and systems engineering lifecycle; and
- Workforce alignment and responsibility to enhance cybersecurity.

While NIST SP 800-37 outlines the general elements of a risk management process, it allows agencies to provide specific guidelines by which to implement it. Accordingly:

- NIST issued SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, which is designed to help organizations develop continuous monitoring solutions. It specifically addresses Step 6 of the NIST SP 800-37 risk management framework on monitoring security controls.
- NIST issued SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, to provide guidelines to organizations when security controls to safeguard their networks as part of a risk-based approach to cybersecurity.
- DHS issued Sensitive Systems Policy Directive 4300A, which outlines specific guidance for DHS components to help implement NIST SP 800-37 on unclassified systems, including TSE.[5] 4300A designates specific controls from NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, to secure its IT systems.[6]
- TSA issued Management Directive 1400.3, *Information Technology Security,* to explain policies and procedures to support the secure use, development, and maintenance of TSA IT systems in accordance with the aforementioned documents.[7]

B.2 Additional Documents Influencing the OSC Cybersecurity Management Framework

OSC reviewed, aligned, and tailored its Cybersecurity Management Framework to several additional Federal policies to meet emerging requirements, as well as other methodologies that highlight mission and organizational priorities.

B.3 DHS Continuous Diagnostic and Mitigation Program

DHS' Continuous Diagnostic and Mitigation (CDM) Program "provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first."[8] DHS CDM Program uses sensors to collect cyber threat information in support of near real-time security monitoring across Federal civilian agency systems, enabling officials to prioritize and mitigate cybersecurity risks. All Federal agencies are required to implement CDM per OMB Directive 14-03, as the *FISMA Act of 2014*.[9,10]

To understand the CDM program and its foundations, the following federal documents reflect the broader goals of federal agencies:

1. The Joint Continuous Monitoring Working Group (JCMWG) Federal Government Continuous Monitoring Concept of Operations;[11]
2. The current fiscal year's Federal FISMA Reporting Metrics;[12] and

[5] DHS, *Sensitive Systems Policy Directive 4300A*. March 2014
[6] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[7] TSA Management Directive 1400.3. *Information Technology Security.* April 2014
[8] DHS. Continuous Diagnostics and Mitigation Program. http://www.dhs.gov/cdm
[9] OMB. Memorandum 14-03. *Enhancing the Security of Federal Information and Information Systems.* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf
[10] Public Law 113-283, FISMA of 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[11] Federal CIO Council. Information Security and Identity Management Committee. https://cio.gov/about/groups/information-security-identity-management-committee/
[12] Published through DHS and OMB.

3. OMB A-130, Management of Federal Information Resources (current version).[13]

B.5 TSA Strategy Documents

- **TSA Strategic Five-Year Technology Investment Plan Report to Congress.** This plan outlines several goals for how TSA can use technology to meet TSA's mission. One of the document's main themes is integrating principles of risk-based security in capabilities, processes, and technologies.
- **TSA Enterprise Risk Management Policy.** This document outlines a risk management process for TSA and determines TSA's risk tolerance based on potential outcomes of the risk.

Alignment to these documents provides the framework with the level of specificity needed to be applicable to OSC's environment

[13] OMB. Management of Federal Information Resources. https://www.whitehouse.gov/omb/circulars_a130_a130trans4/