Security Technology Integrated Program (STIP) 101

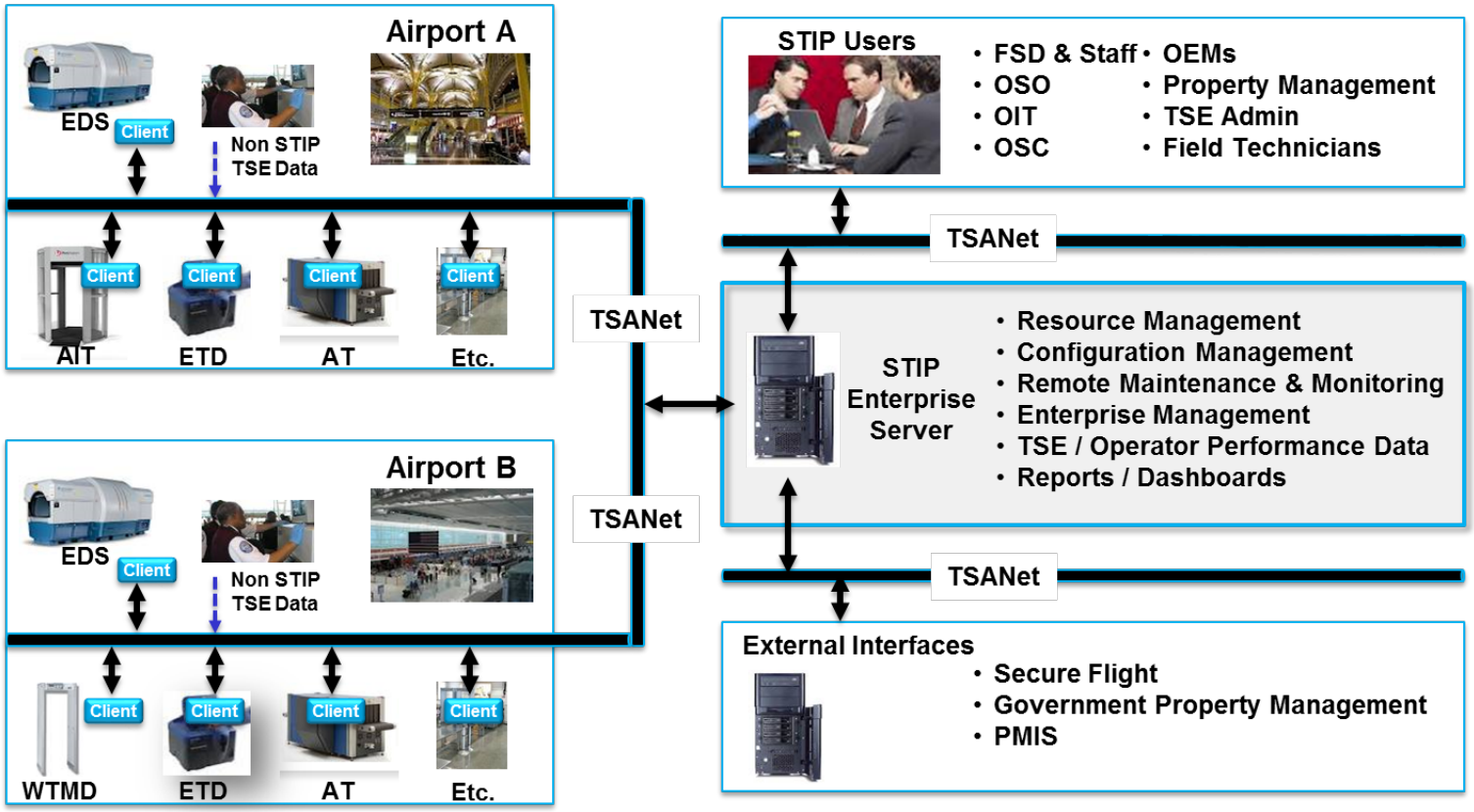
May 2016

Transportation Security Administration

OSC
Office of Security Capabilities

STIP Connectivity Overview

STIP System Boundary consists of STIP-enabled TSE at airports connected to the STIP Enterprise Server. STIP users and external interfaces (e.g., Secure Flight, GPM) send and receive data to the STIP Enterprise Server, while data communication between the STIP system is through TSANet.



Transportation Security Administration

All TSE are currently disconnected from TSANet due to cybersecurity requirements imposed by the Department of Homeland Security (DHS)

OSC
Office of Security Capabilities

Goals and Capabilities of STIP

Security Technology Integrated Program (STIP) provides a dynamic and adaptable communications infrastructure that facilitates the transfer of data to and from Transportation Security Equipment (TSE) on the TSA Network.

Goals

Improve Information Management

STIP collects and disseminates critical data related to TSE, improving situational awareness and risk-based decision making processes.

Improve Security Agility

STIP enhances TSA's ability to respond to emerging threats by remotely pushing software and other configuration changes to TSEs.

Increase Operational Efficiency

STIP enables TSA to remotely monitor, diagnose, troubleshoot, and manage TSE, allowing TSA to address equipment issues and prevent failures.

Decrease Total Cost of Ownership

STIP allows OSC to realize major cost benefits as TSE configuration, data collection, and maintenance are streamlined to reduce on-site visits.

- **Streamlined Operations**
- **Security Flexibility**
- **Greater Efficiencies**

Capabilities

Enterprise Management	Configuration Management	Resource Management	Equipment Maintenance
• Automation of data collection from Transportation Security Equipment (TSE) • Automated reports and dashboards that provide holistic views of equipment performance	• Accurate verification and tracking of configuration settings (e.g., for Threat Image Projection) • Configuration audit of approved baseline to ensure that deployed TSEs are performing per original spec.	• Automated TSE asset inventory tracking • TSE usage tracking • Automated tool for Change Control Board (CCB).	• Remote diagnostics • Reduced TSE downtime • Eliminates redundant maintenance visits

Credential Authentication Technology (CAT)

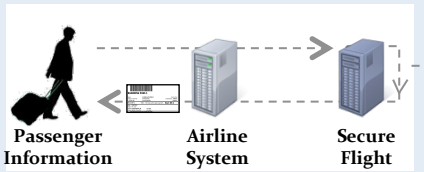
The networked CAT solution (CAT Phase II) relies on network connection to Secure Flight via STIP in order to receive passenger flight and vetting information.

Networked CAT Solution with STIP

Pre-Checkpoint Operations

Passenger Pre-Screening

Passenger risk is determined by Secure Flight and communicated to CAT through STIP.



- Passenger provides data to SecureFlight (SF)
- SecureFlight conducts vetting and returns result to airline
- Passenger accesses boarding pass

Checkpoint Operations

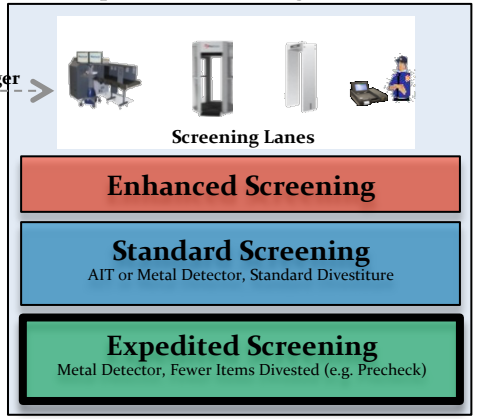
Boarding Pass Assessment

The passenger's BP and ID are compared to ensure that they are directed to the correct screening.

- Credential Authentication Technology (CAT) validates ID
- CAT displays passenger vetting status information to TSO
- TSOs directs passenger to lane

Physical Screening

The passenger undergoes physical screening processes by Transportation Security Officers.



Benefits

- Ability to access and vet passengers through SecureFlight at the checkpoint
- Authentication of IDs
- Risk-based security approach at the checkpoint
- Encryption of PII data in transit

Transportation Security Administration

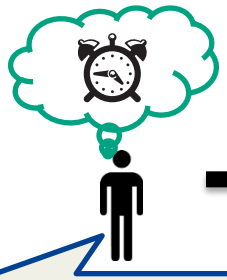
Passenger pre-screening expedites current passenger screening while increasing the scrutiny of higher-risk passengers

OSC Office of Security Capabilities

TSE Data Automation

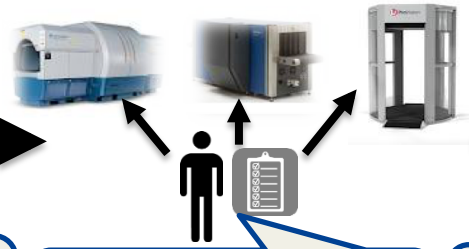
Challenges Associated with the Current TSE Data Collection Process

(1) Data collection occurs every hour



Inconsistency in timeliness of data collection.

(2) Transportation Security Officers (TSO) manually record data from TSEs

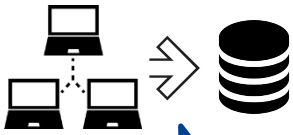


Inaccurate data collected from human error in hourly data recording.

(3) TSOs manually enter captured data into computer

Human error in typing data into computer and lack of robust data entry verification.

(4) The airport coordination center inputs data daily into PMIS



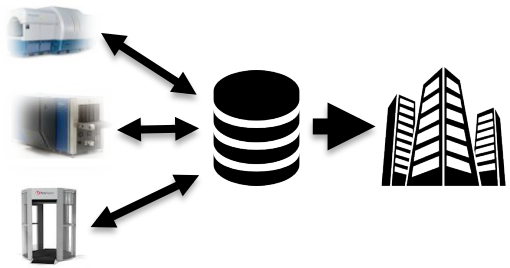
Error in transferring data into PMIS.

(5) The data is accessible by various stakeholders

Substantial delays in information processing due to the complex data dissemination process.

Benefits of STIP with the TSE Data Collection Process

The Enterprise Manager will automatically collect STIP-enabled TSE data and interface directly with the PMIS database.



- ✓ STIP allows for improved accuracy in timing of data collection.
- ✓ STIP will allow data to be transmitted with improved accuracy directly to the PMIS database, thereby eliminating any intermediate steps in the data processing chain.
- ✓ STIP will allow for significant time savings in the data collection process.

Transportation Security Administration

Average time savings per TSE per day = 11.7 minutes
~300 FTE savings in FY16 increasing to ~550 FTE savings in FY20 and beyond.

OSC
Office of Security Capabilities

Remote Monitoring and Maintenance (RMM)

Challenges Associated with the Current TSE Maintenance Process

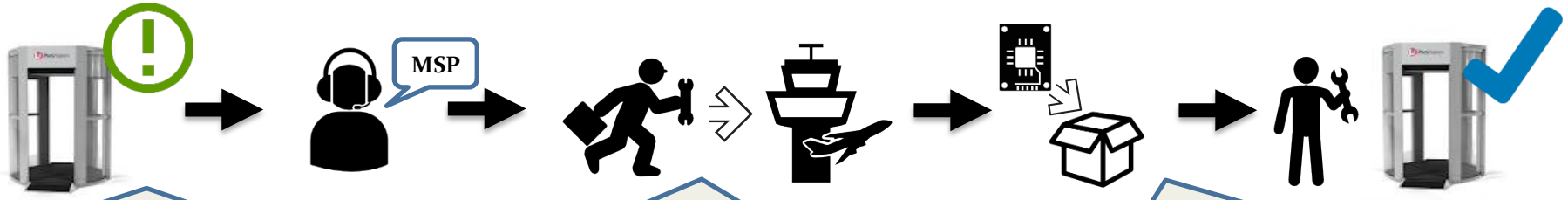
(1) TSE requires maintenance

(2) The Maintenance Service Provider (MSP) is alerted of the issue by local TSA

(3) Field Service Technician (FST) travels to the airport to assess and diagnose the issue

(4) Necessary parts and equipment are ordered

(5) FST travels back to the airport, repairs the TSE, and notifies local TSA of completion



Maintenance ticket data for under warranty and out of warranty was provided by ILS.

Time difference between dispatch and the start of diagnostics was calculated.

FSTs would travel twice to the airport for tickets requiring a part.

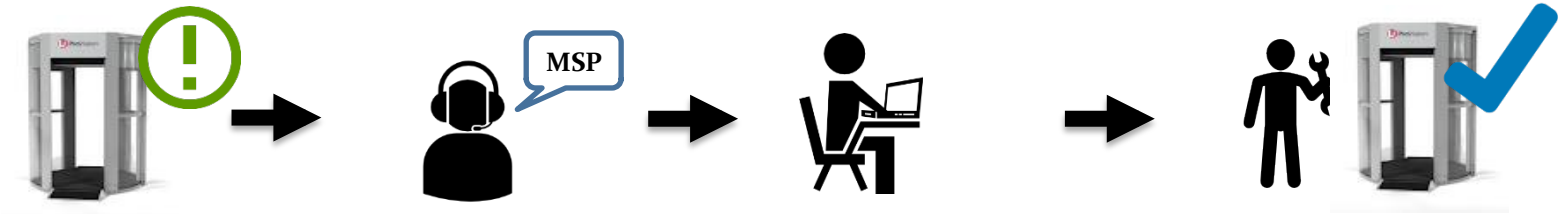
Benefits of STIP with the TSE Remote Monitoring and Maintenance Process

(1) TSE requires maintenance

(2) The Maintenance Service Provider (MSP) is alerted of the issue by local TSA

(3) The FST remotely diagnoses the issue, orders parts, and only travels to the airport once for maintenance

(4) FST arrives at airport, repairs the TSE, and notifies local TSA of completion



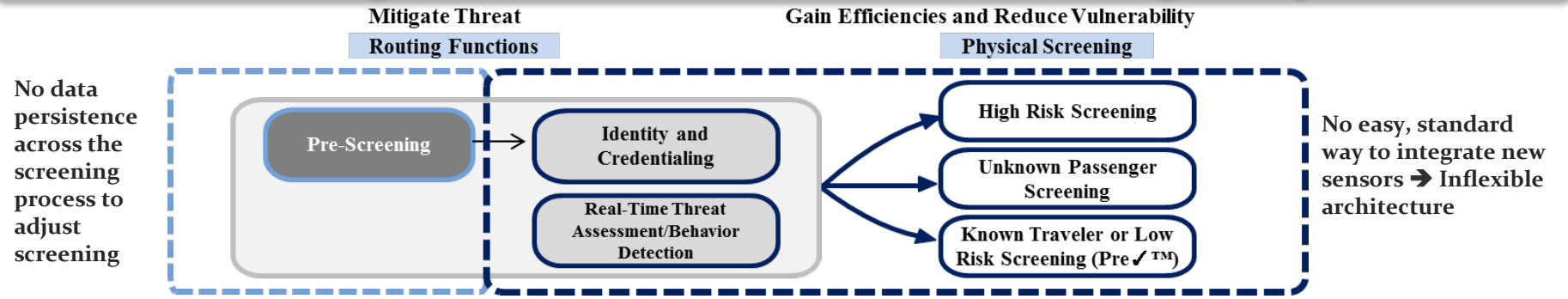
Transportation Security Administration

The average time savings for one TSE per year = 3.25 hours

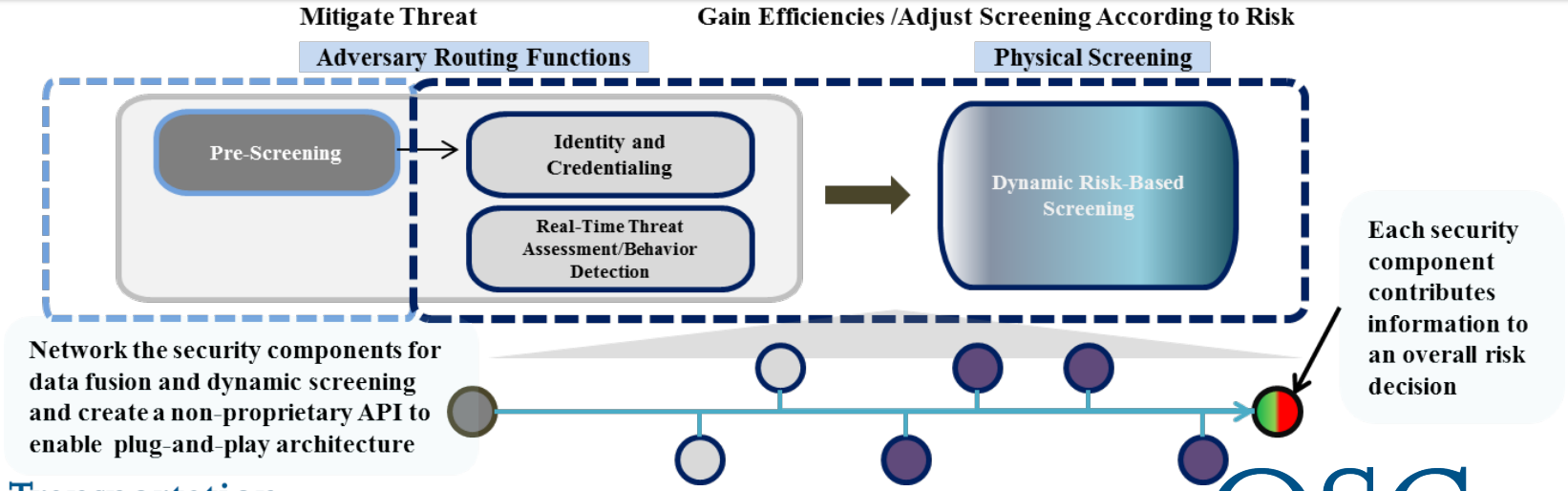
OSC Office of Security Capabilities

Future State:
Dynamic Risk-Based Screening (RBS)

Challenges Associated with the Current RBS Screening Concept



Introduce an API and IT architecture

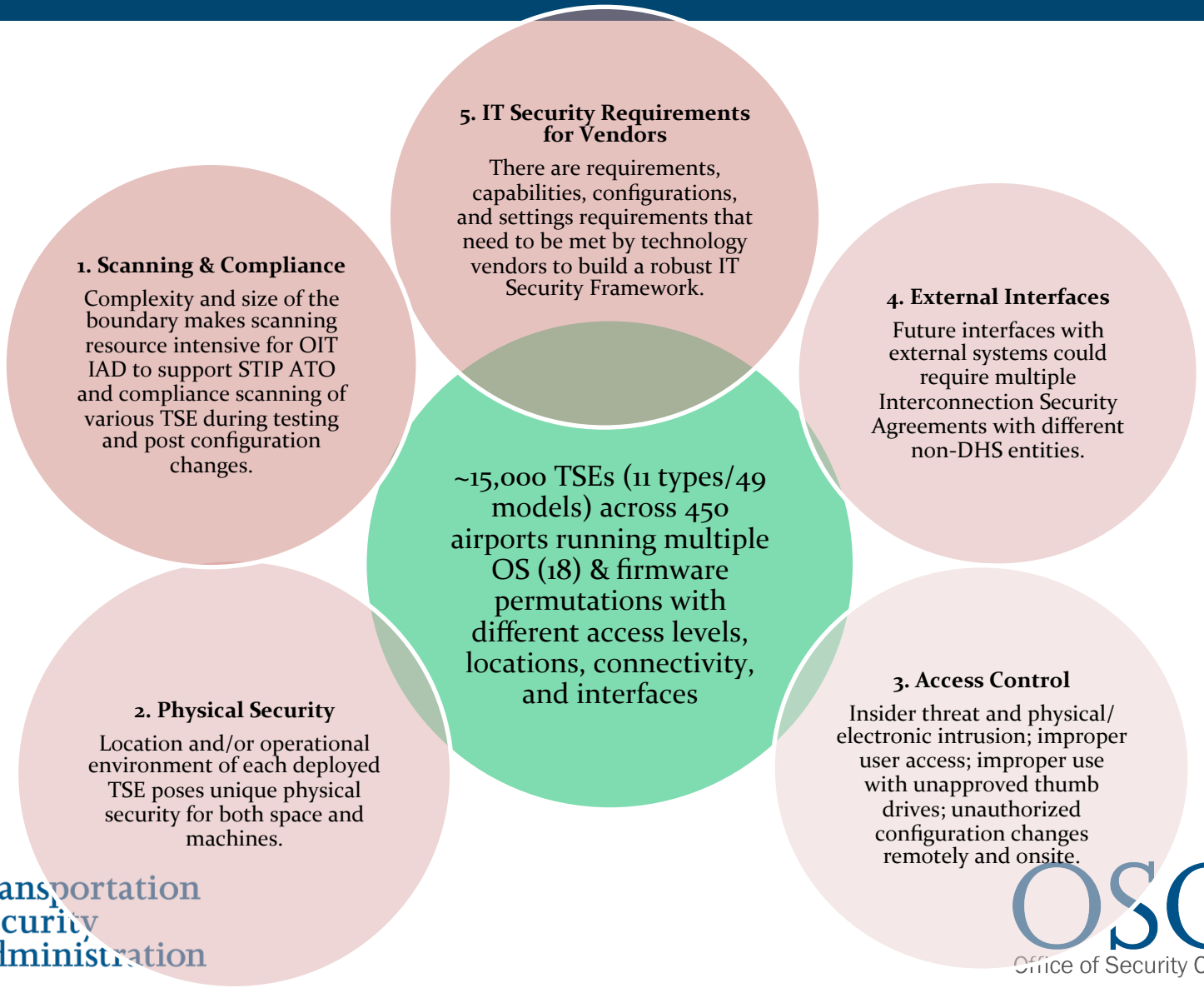


Allows for data persistence, data fusion, and dynamic physical screening based on risk and will enable Dynamic RBS

Transportation Security Administration

OSC Office of Security Capabilities

Five IT Security Challenge Areas for TSE Environment



TSE Cybersecurity Requirements
(End-points)

TSA identified nine (9) IT security requirements to enforce cybersecurity compliance of legacy and future TSE. TSE must comply with all (9) requirements prior to reconnecting to STIP.

OS Currency/Security Patching	• All TSE operating systems (OS) shall be patched to current OS vendor-supported versions when first delivered. Patches will be updated every 30 days. For critical vulnerabilities, the Original Equipment Manufacturer (OEM) will patch per the prescribed time window as determined on a case by case basis.
OS Hardening	• All TSE shall be compliant with the approved DHS Hardening Guidelines for the platform on which they are being developed.
AV Updates	• TSE shall include TSA-approved anti-virus (AV) software configured to receive digitally signed automatic AV virus definition file updates remotely.
PIV Compatibility	• All privileged TSE users shall be vetted by TSA's Personnel Security Division and audited by IAD annually. Privileged users shall use Personal Identity Verification (PIV) cards issued by TSA to access the TSE. Vendors will be required to make their TSE compatible with TSA-issued PIV.
Security Scanning Support	• In support of OSC's efforts to ensure devices are compliant with all IT Security requirements, TSE will be assessed and scanned by the OIT IAD. OEM technicians to be on-site as necessary to provide access to the TSE.
Technical Obsolescence	• All TSE contracts shall include technical obsolescence clauses that mandate the upgrade and/or replacement of any software or hardware components that are considered to be Configuration Items that are no longer actively supported by the manufacturer.
SOC Monitoring	• All TSE endpoints shall be monitored by the TSA Security Operations Center (SOC). TSE shall include TSA-approved Continuous Diagnostics and Mitigation (CDM) software configured enable SOC monitoring.
POA&M Support	• Upon completion of security scans, findings will be documented and categorized as high, medium, or low based on their potential impact to the TSE IT Security posture. OEMs will support the remediation of open Plan of Action and Milestones (POA&M) items in a timely manner.
Vendor ISSO Designation	• If TSA has procured Full-Rate Production (FRP) TSE from an OEM, then the OEM will be required to have a designated Information Systems Security Officer (ISSO) to coordinate with OSC ISSOs on IT Security issues.

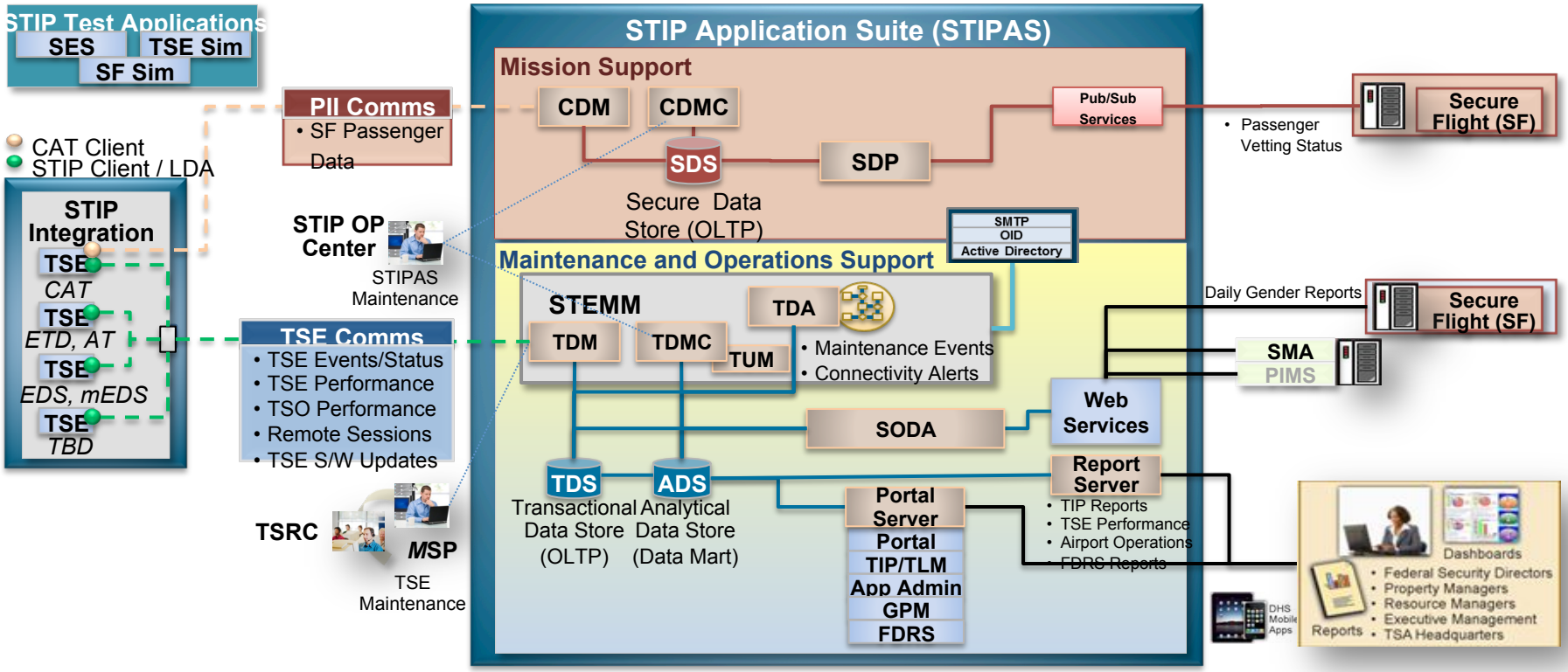
Transportation Security Administration

OSC has stood up a Cybersecurity Mediation Integrated Project Team (IPT) with OIT, OA, and OSO to address cybersecurity concerns and challenges

OSC
Office of Security Capabilities

STIP 3.0 Architecture

The diagram below highlights the interaction between TSEs and the STIP Application Suite (STIPAS).



New architecture: increased scalability, performance and the openness of the STIP architecture, allowing it to comply better with TSA Enterprise Architecture standards.

New Data Sharing Layer: standardized/enhanced STIP's ability to share TSE data with external systems.

CAT support: Successfully validated SF-STIP-CAT data flow using prototype CAT machines.

STIP 3.0 implemented **Public Key Infrastructure (PKI) certificates** for communication between the TSE and the Enterprise components of STIP for a more secure solution.

STIP 3.0 application portal will be architected to support future **Personal Identity Validation (PIV) card 2-factor validation**.

STIP enhanced **encryption level** from 128 to 256.

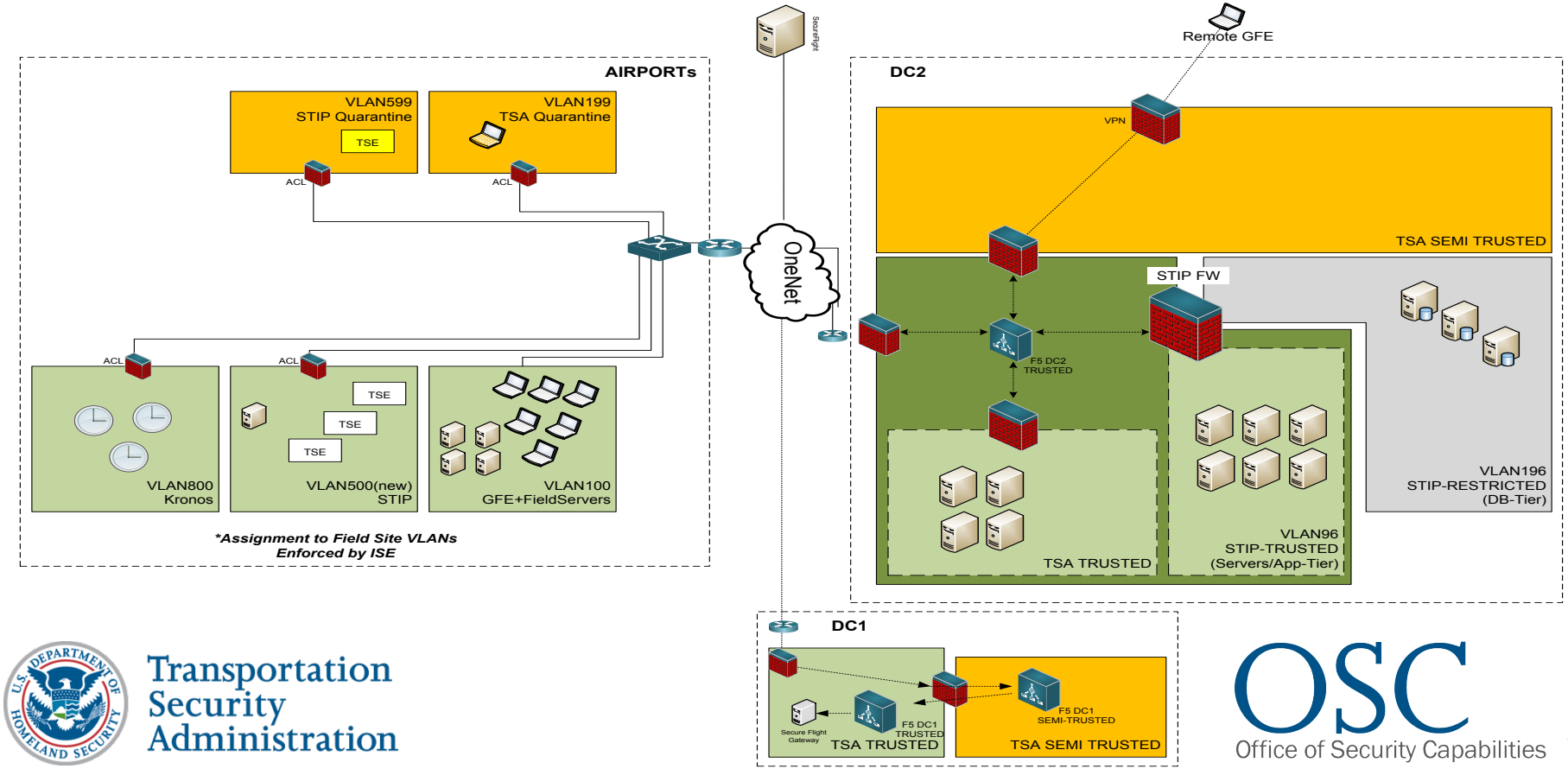
Transportation Security Administration

OSC Office of Security Capabilities

STIP Network Segmentation
(Back-end Infrastructure)

OSC and OIT discussed four proposed solutions for TSE network connectivity and determined segmentation as the most effective path forward. The following diagram outlines the key components of the solution:

- Cisco Identity Services Engine (ISE) will be used to enforce rules, keeping TSEs on their own VLAN and using ISE agents
  - STIP databases will relocate from TSA Operating Platform (TOP) to STIP's own database hardware
  - STIP at Data Center 2 (DC2) will segment onto its own Trusted VLAN
  - STIP will inherit new database backend servers and a new Restricted VLAN



Transportation Security Administration

OSC Office of Security Capabilities