Security Technology Integrated Program (STIP) Cybersecurity

May 2017

Transportation
Security
Administration

Office of
ACQUISITION Program
Management

Disclaimer

This is not a Q&A for DOMAIN

Search HSTS04-17-I-STAD01 on the FBO website

Contact

Kerry Toscano - kerry.toscano@tsa.dhs.gov

Kyra Fromeke - kyra.froemke@tsa.dhs.gov

TSE Cybersecurity Requirements
(End-points)

TSA identified nine (9) IT security requirements to enforce cybersecurity compliance of legacy TSE. Future TSE must comply with all apporiate requirements prior to reconnecting to STIP. Monitoring/scanning will be automated in the future.

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 OAPM'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

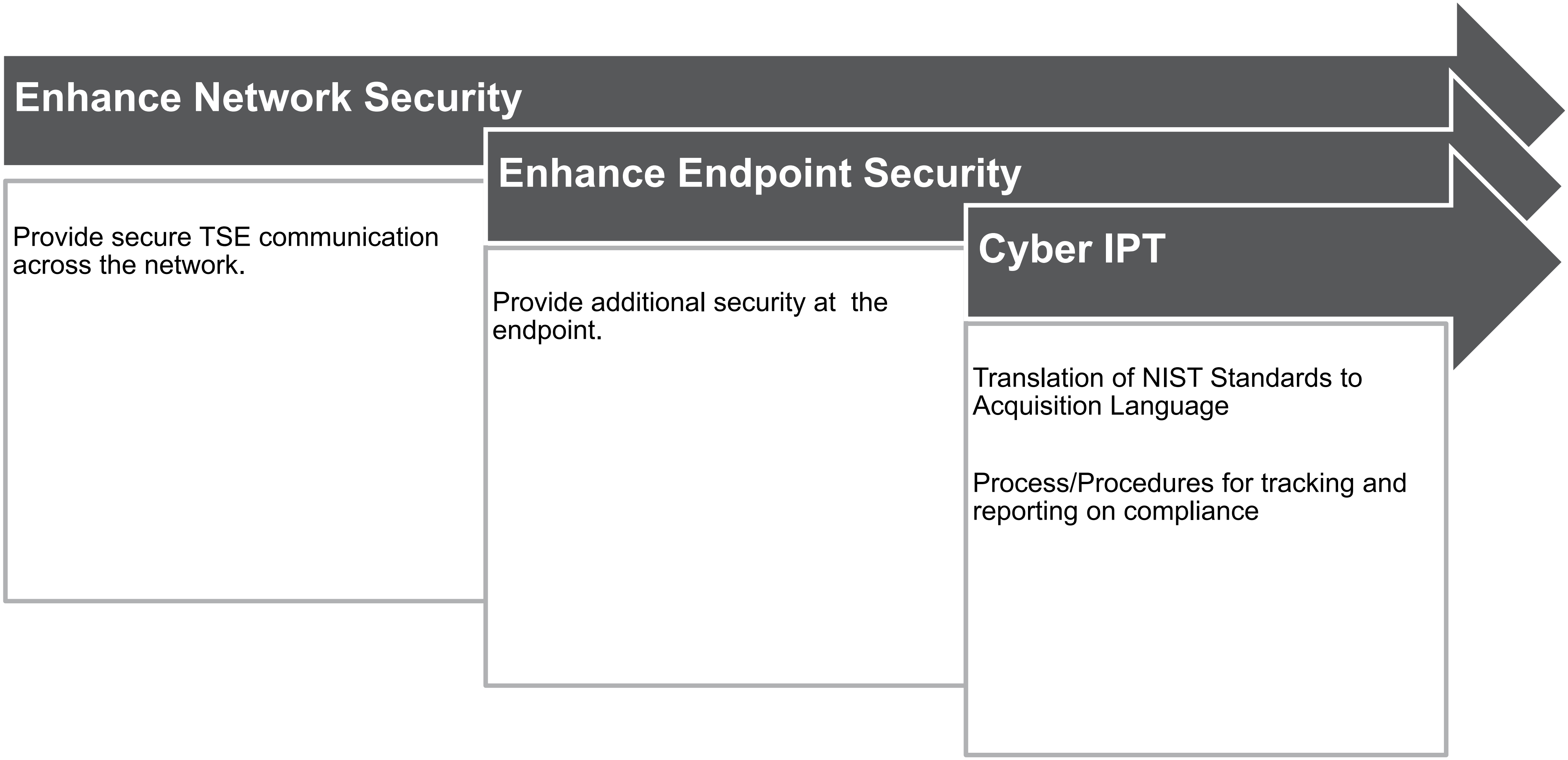
- If TSA has procured Full-Rate Production (FRP) TSE from an OEM, then the OEM will be required to have a designated Information Systems Security Officer (ISSO) to coordinate with OAPM ISSOs on IT Security issues.

Transportation
Security
Administration

OAPM has stood up a Cybersecurity Integrated Project Team (IPT) with OIT and OAPM to address cybersecurity concerns and challenges

Office of ACQUISITION Program Management

Path Forward



Enhance Network Security

Provide secure TSE communication across the network.

Enhance Endpoint Security

Provide additional security at the endpoint.

Cyber IPT

Translation of NIST Standards to Acquisition Language

Process/Procedures for tracking and reporting on compliance

Questions

1. **How real are cyber threats?**

Response: Cyber threats are very real! Especially if TSEs are considered as another class of Internet of Things (IoTs). Attacks against IoTs are now more pervasive and sometimes, massively successful, that can turn these devices into bots used to launch other types of attacks such as DDOS (Mirai botnets come to mind). If TSEs are ever put on a network that have little to no security controls in place, there is a high likelihood that these devices will get compromised. Also remember that even in its unconnected state, infection from USB thumb drives plugged into it is a risk and a viable attack vector as well. Remember STUXNet? The other factor that contributes to the realism of cyber threats is the amount of open source malicious information available on the internet. Any person can conduct a Google search to find entire libraries of malicious code as well as “how to” guides all free for download to exploit IoTs and unsecured networks.

2. **What is the impact of a cyber attack?**

Response The impact of a cyber-attack on TSE’s could range from frustrating to catastrophic. We have spent some time considering various “nightmare scenarios” that could arise from a successful attack on TSE’s. These scenarios include

- Injection of “clean” scan results on a bag containing dangerous weapons/explosive materials
- Injection of “dirty” scan results on a “clean” bag/item to slow a checkpoint.
- Injection of “dirty” scan results on all “clean” bags/items to shut down entire checkpoints/airports.
- Theft of scanning parameters to reverse engineering current capabilities and create mechanisms to escape detection.

Questions

3. **What can be done to protect TSE, but not by hardening the TSE itself? E.g., removing TSE from networks or using private networks?**

Response A few suggestions:

- TSEs should be on a dedicated purpose built network with device access controls and highly secured, locked down and tightly controlled gateways connecting back to TSA
- Block unneeded ports and monitor ALL traffic to and from the TSEs
- Have a patching plan in place and regularly patch all TSEs
- Create strong authentication for all TSEs that need to communicate to other TSA systems and devices outside of its dedicated network

4. **Can TSE be safe if it is connected to a TSA or public networks?**

Response No. Not in our opinion.