

*How the DHS CISO is Implementing  
The Blueprint for a Secure Cyber  
Future: The Cybersecurity  
Strategy for the Homeland  
Security Enterprise*

*Protecting the Information that Secures Our Homeland*



**Homeland  
Security**

DHS OCISO

# Focus on Goal 4-1 QHSR

Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment. Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's digital infrastructure. Understand and prioritize cyber threats. Identify and evaluate the most dangerous threats to federal civilian and private-sector networks and the Nation.

## Objectives:

Manage risks in cyberspace. Protect and make resilient information systems, networks, and personal and sensitive data.

Develop a robust public-private cyber incident response capability. Manage cyber incidents

Prevent cyber crime and other malicious uses of cyberspace. Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.

Develop a robust public-private cyber incident response capability. Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.



# Creating a Safe, Secure, and Resilient Cyber Environment to Support the Homeland Security Missions

## Improving Resilience

### Core capabilities for the homeland security enterprise are:

- ✓ Comprehensive understanding of vulnerabilities, critical dependencies, and interdependencies.
- ✓ Architectural guidance and standards for resilience.
- ✓ Conformance to established resilience standards and guidelines.
- ✓ Methods to create diversity in software systems and networks.
- ✓ Continuous audit.



# Policy

- Policy to address topics such as cloud computing, social media, digital signatures, common control catalogs, use of PIV, TRM, Standards (CVE, OVAL, CPE, etc.), Supply Chain Threats, Compliance.
- Manage dynamic security policy waiver and exception program to meet unique mission requirements

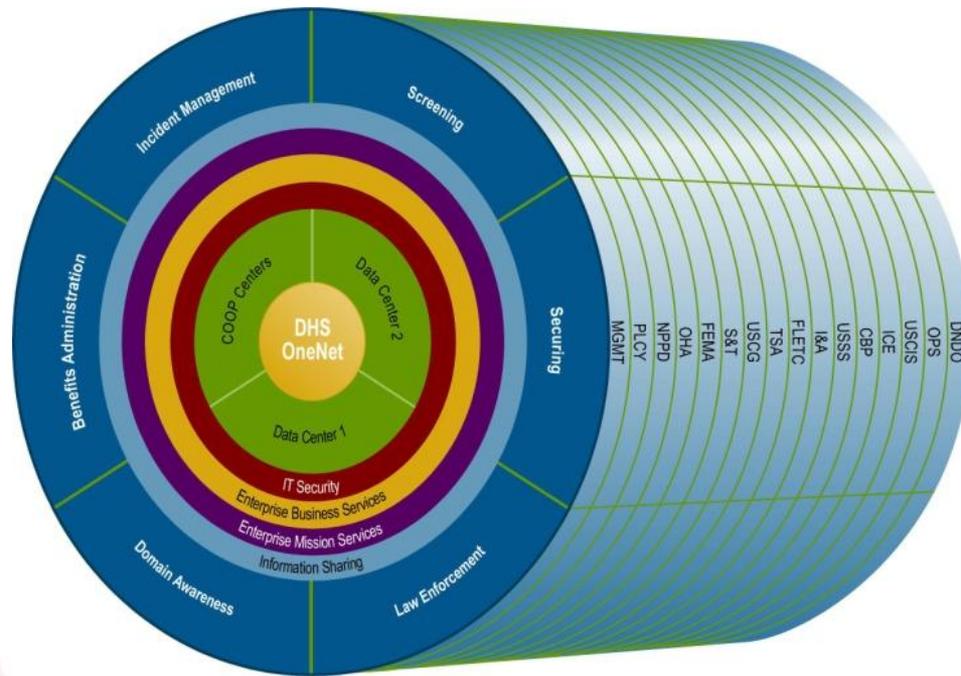


# Focused Operations

- Conduct classified operations to detect and respond to the Advanced Persistent Threat (APT)
- Focused Ops analysts work with the Security Operations Center to correlate intelligence information with SOC data to identify APT attacks, mitigate the effects, and develop countermeasures to ensure the protection of the Department's mission critical systems

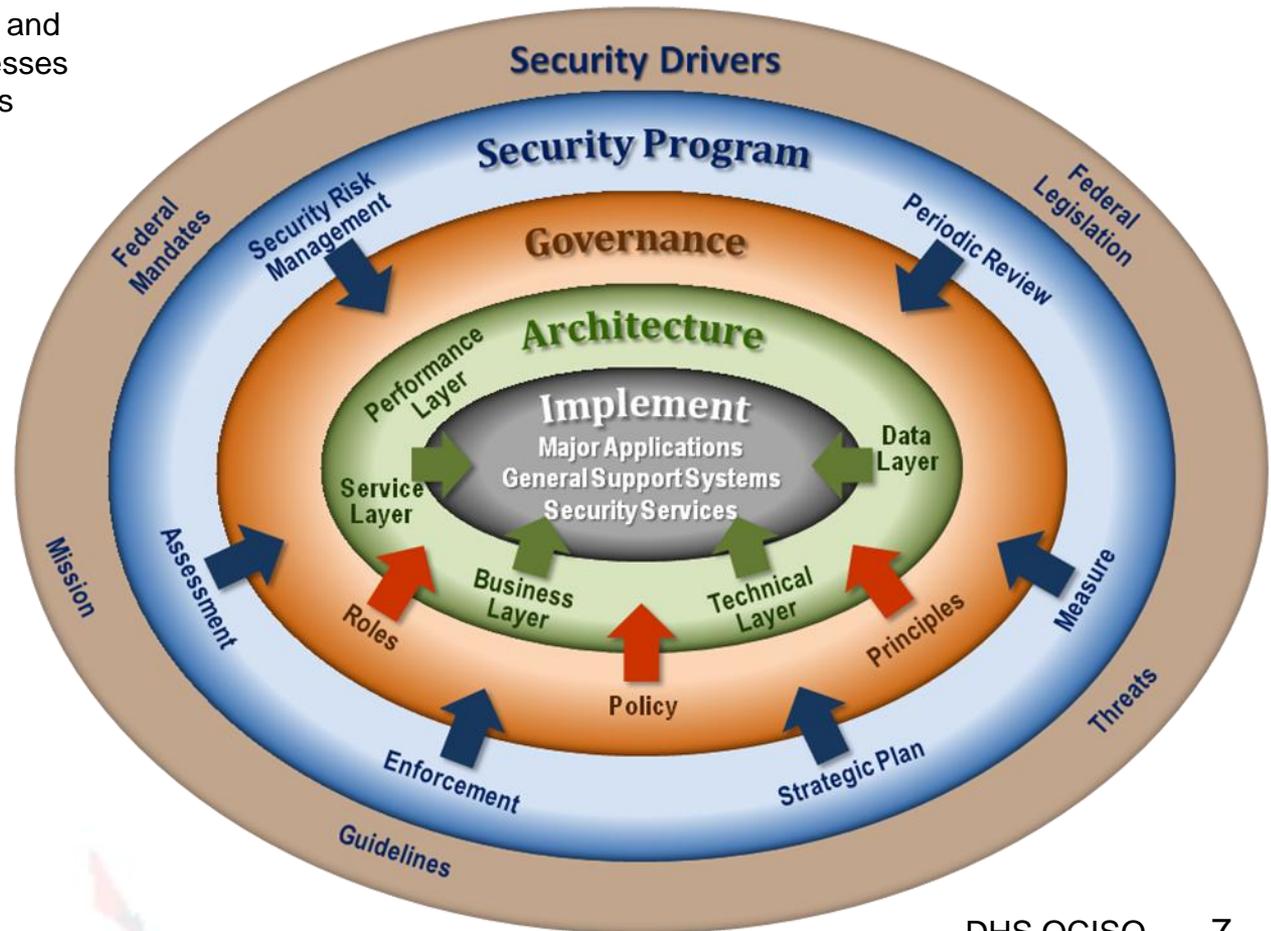


# Security Architecture

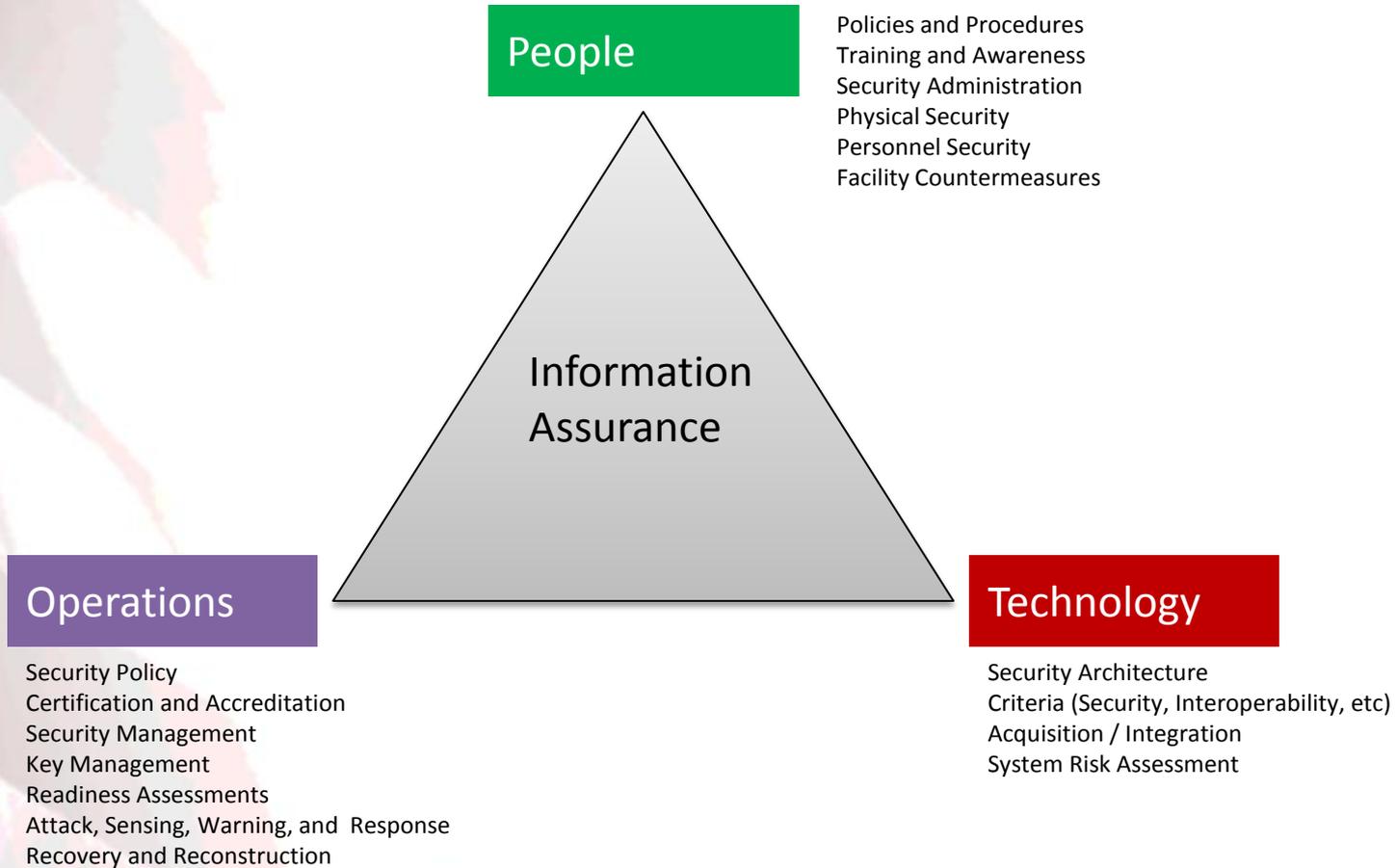


# Security Architecture Approach

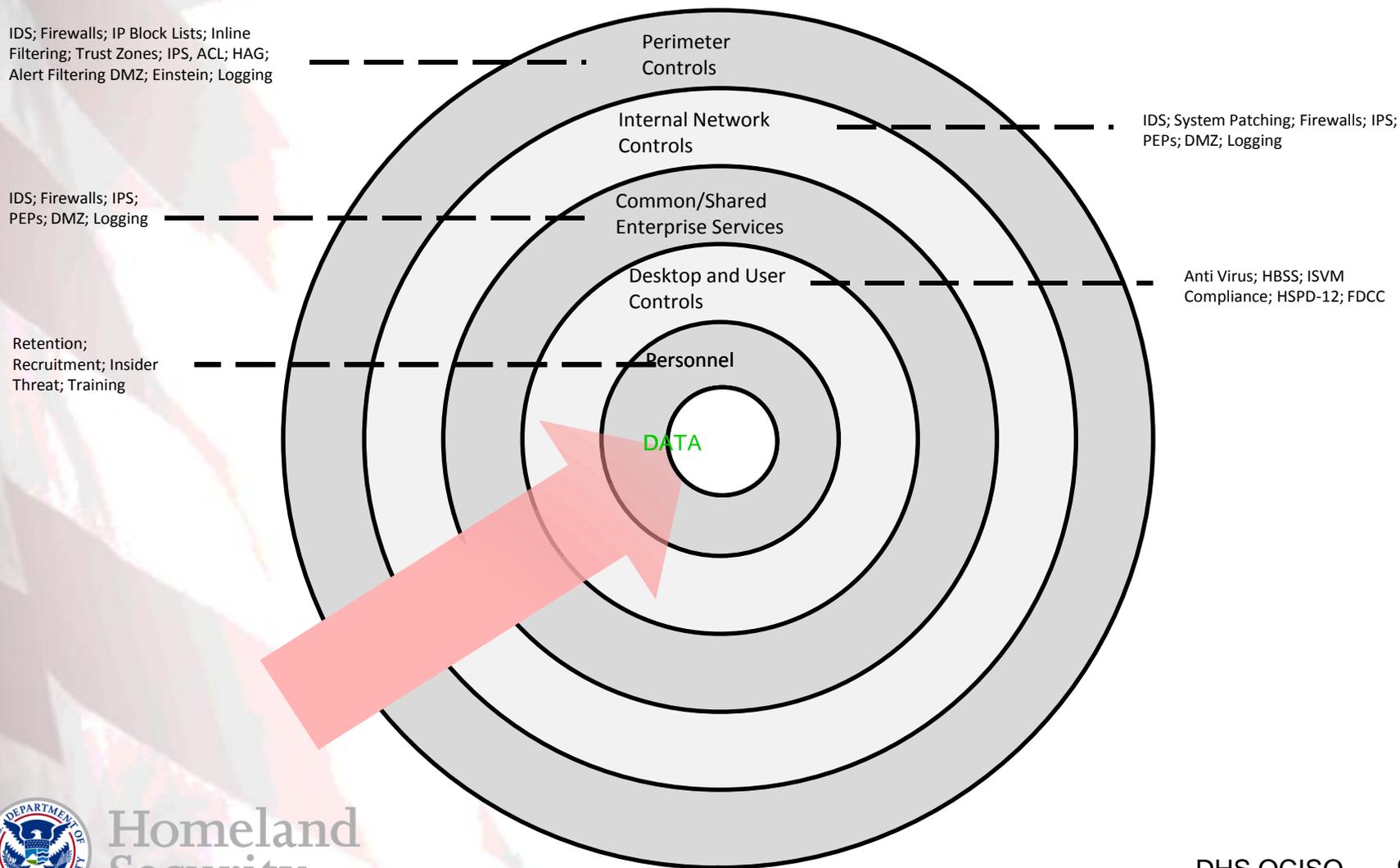
- Enterprise life-cycle approach for Security Architecture that supports the DHS mission.
- Holistic approach in which architecture input and output were considered and identifies the major security processes and security architecture elements affected by these processes.



# Security Architecture Strategy



# Security Architecture Layers



# Cyber Preparedness Levels

Levels	Cyber Threat	Cyber Prep
5 Cyber Warfare	<u>Advanced</u> : e.g., peer nation military; Very sophisticated, entrenched, persistent adversaries; insidious, coordinated, Internet, insider, supply chain, and physical attacks over the long term; Intent: destroy org's mission capability in support of broader objective.	<u>Pervasive Agility</u> : Apply agility, adaptation, and flexibility to all aspects of organization to dynamically reshape all aspects of operations despite adversary actions.
4 Cyber Espionage	<u>Significant</u> : e.g., intelligence service; Sophisticated adversaries, with persistent footholds within the org's infrastructure; primarily Internet and insider attacks, intent is intelligence gathering, placing sleeper components, and impeding critical operations.	<u>Architectural Resilience</u> : Ensure mission operations (albeit degraded) despite adversary gaining foothold and launching attacks.
3 Cyber Surveillance	<u>Moderate</u> : e.g., terrorist cell; Adversaries with significant expertise, seeks to gain foothold in the org's infrastructure for purposes of exfiltrating critical data.	<u>Responsive Awareness</u> : Monitor for and defend against attacker gaining foothold.
2 Cyber Crime	<u>Limited</u> : e.g., thieves; Adversaries with some technical expertise; cybercrime intent; opportunistic attacks to acquire information	<u>Critical Information Protection</u> : Protect information regardless of form or location.
1 Cyber Vandalism	<u>Unsophisticated</u> : e.g., hackers; Generic adversaries; non-targeted attacks, primarily focused on enterprise perimeter; intent is defacement or self aggrandizement.	<u>Foundational Defense</u> : Protect organization systems at the perimeter.



\* Mission Assurance and the Art of Cyber Defense – MITRE Harriett Goldman

# Representative Security Measures

5	<p>Strong I&amp;A for all access</p> <p>Near-real-time forensics</p>	<p>Integrated cyber &amp; physical PEN testing</p> <p>Dynamically changing hardware &amp; software</p> <p>Virtualization to reconstituting services</p>	<p>Contingency reserve</p> <p>Use multiple suppliers for key components</p>	<p>Code analysis</p> <p>Trusted cutouts to support shipping</p> <p>Use of trusted components</p>
4	<p>Strong I&amp;A for local access to critical ISs</p> <p>Network segmentation</p>	<p>PEN test physical security</p> <p>Heterogeneous OSs</p> <p>Thin clients</p>	<p>Purchase spare parts up front</p> <p>Use trusted shipping</p> <p>Two-person rule</p>	<p>Plan for degraded mode operation</p> <p>Make frequent changes to s/w and h/w</p>
3	<p>Strong I&amp;A for all privileged access</p> <p>Network behavior, analysis &amp; detection on internal network</p>	<p>Correlate physical &amp; cyber access</p> <p>Honeyclient</p> <p>Honeypots</p> <p>Monitor internal audit logs</p>	<p>Integrity checking internal systems</p> <p>Rootkit detection</p>	<p>Identify potential cyber attack areas</p> <p>Deploy sensors at critical points to detect exfiltration</p> <p>Monitor control channels through perimeter</p>
2	<p>Strong I&amp;A for all external communications</p> <p>Redundancy of external systems</p>	<p>Physically secure critical systems</p> <p>Segregated DMZ</p>	<p>Scan portable systems</p> <p>Periodic open source searches</p>	<p>Encrypted external transmissions</p> <p>Full disk encryption</p> <p>Wireless &amp; PED encryption</p>
1	<p>Strong I&amp;A for remote privileged access</p> <p>Assessment of external systems</p>	<p>Perimeter intrusion detection</p> <p>Perimeter firewalls</p>	<p>Security patching</p> <p>External network scanning</p>	<p>Anti-virus on email &amp; client systems</p> <p>Audit log monitoring</p>

# Cyber Threat

***Focused Operations Analysis*** – Identification, collection, examination, correlation, analysis, and documentation of data from multiple DHS Information Infrastructure sources fused with appropriate information available from other Computer Network Defense (CND), Intelligence Community (IC) and Law Enforcement/Counterintelligence (LE/CI) sources.

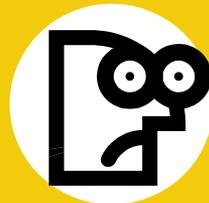
***Cyber Threat Analysis*** – Provide near real-time intelligence/situational awareness support to Focused Operations Analysts (CTAC and SOC) as well as senior OCIO leaders (CIO, CISO, DIRSOC, etc.) and fuse Focused Operations (FO) information with other Computer Network Defense (CND), Intelligence Community (IC) and Law Enforcement/Counterintelligence (LE/CI) Cyber Communities of Interest (COI) sources.

***Digital Media Analysis*** – Acquisition, authentication, reconstruction, examination, analysis and technical reporting of data stored on electronic media.

***Liaison Officers*** - Representatives from CTB to NPPD/NCCIC and I&A/CIPD as a technical liaison and advisor on DHS Information Infrastructure cyber security matters. Represents the DHS OCIO (CIO, CISO, ITSO & DHS SOC).

***Focused Operations Joint Task Force*** – Representatives from component SOC/FO shops meet regularly to exchange information concerning FO analysis/reporting.





**It's QUESTION TIME!!**



Homeland  
Security