NIST-DHS High Value Asset Control Overlay

Federal Network Resilience (FNR)
Cybersecurity Assurance Branch (CAB)

Date: June 1, 2017
Discussion Topics

• What is an High Value Asset (HVA)
• M-17-09
• Security Architecture Reviews
  – Common Findings / Risks
• Common Threats
• HVA Overlay & Models
  – Privacy Overlay
  – CNSSI No. 1253
  – NIST SP 800-82 Guide to ICS Systems
• Bounds for Overlay Document
• HVA Overlay Control Families
• Categorization & Control Selection Challenges
  – FIPS 199 & 200
  – Beyond FIPS 199 & 200
• Notional Timeline
What is an HVA?

• HVAs are not the typical IT system because these are critical to support our federal mission – AKA “Crown Jewels”

• M-17-09:
  – "High Value Assets" are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government.
M-17-09 Risk Assessment Requirements

• HVA risk assessment scope and stakeholders beyond IT
  – incorporate operational, business, mission, and continuity considerations.

• Interconnected Risk:
  – interdependencies leading to significant adverse impact on the functions, operations, and mission of other agencies.

• Risk Assessments Informed By:
  – up-to-date awareness of threat intelligence regarding agencies' Federal information and information systems;
  – the evolving behaviors and interests of malicious actors; and,
  – the likelihood that certain agencies and their HVAs are at risk due to adversary interest in agencies' actual, related, or similar assets.
Common Risk Examples

- **Governance & Risk Management** – understanding the agency’s strategy for managing risk and oversight (mostly with federated agencies).
- **System Boundary** – understanding the conceptual scope of the HVA environment and the protections required to secure it (control tailoring, inheritance).
- **Network Segmentation** – separating (logically or physically) components based on criticality and trustworthiness, to limit the spread of damage in the event of a compromise (lateral movement).
- **Identity & Access Management** – management, utilization, and safeguarding of identity credentials / information and the resources they access.
- **Continuous Monitoring** – near real-time monitoring of system components and access to support security operations, incident management, and risk management (applications, databases, networks, users, endpoints, etc.).
- **Other** – encryption (at rest/in transit), FIPS 199 categorization, FISMA documentation, diagrams, POA&M management, interconnected risk to other agency system.
Common Threats to Information Systems

- Phishing / Spear Phishing
- Malware
- Credential Scrapping & Escalation
- Lateral Movement inside the network
- Interconnected Risk
- Insider Threat
• Why do we need a control overlay for HVAs?
• Overlay Models
  – **CNSSI 1253** departs from FIPS 200 High Water Mark and looks at decoupling C, I, A to apply controls at a granular level.
  – **Privacy Overlay** provides multiple baseline independent overlays to protect PII.
  – **SP 800-82 Guide to ICS Security**– provides guidance on protecting industrial control systems, distribution control systems.
• All systems declared and identified as HVAs must be moderate impact security control baseline or higher.
• Intended to provide tailoring guidance to agencies to secure HVAs to the degree necessary to protect HVA Information.
• Support additional inputs beyond FIPS 199 to inform agency risk management decision making to ensure applied controls are tailored to provide robust security posture for HVAs.
  – Threat modeling
  – Forecast data exfiltration / breach response costs
• Cost effective approach to applying granular controls to secure HVAs.
HVA Overlay Control Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Identification and Authentication
- Program Management
- System and Communications Protection
- System and Information Integrity

- DHS and NIST are collaborating on these controls to review and validate based on threat and assessment information.
Planning
April / May

Limited SME Review
August

Initial Draft
July

Final Draft
Rev Sept

Release HVA Overlay at same time as 800-53 rev 5

2017