CISA
CYBER+INFRASTRUCTURE

CISA INSIGHTS CYBER

Secure High Value Assets (HVAs)

AT-A-GLANCE RECOMMENDATIONS

- Establish an Organization-Wide HVA Governance Program
- Identify and Prioritize HVA Information Systems
- Consider the Interconnectivity and Dependencies of HVA Systems When Determining Which Systems Are HVAs
- Develop a Methodology for Prioritizing HVAs Based on Criticality and Mission Importance
- Develop an Assessment Approach Based on HVA Prioritization
- Ensure Timely Remediation of Identified Vulnerabilities

CYBERSECURITY THREAT

A High Value Asset (HVA) is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical operations, or they may house unique collections of data. These sensitivities make HVAs of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence by the public.

To counter dynamic threats to the security and resilience of HVAs, it is essential that organizations take a more comprehensive view of the risk they pose and the information and information systems they target.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages its State, Local, Tribal and Territorial (SLTT) government partners, as well as private sector owners of critical infrastructure, to use this guide to learn more about the threat to HVAs and associated mitigation activities. This guidance is derived from Binding Operational Directive 18-02 – Securing High Value Assets and includes lessons learned and additional considerations for non-federal entities seeking to implement actions in line with federal civilian departments and agencies, as directed by CISA.

RECOMMENDED ACTIONS

To address the significant risks to HVAs, CISA directed federal civilian agencies to undertake the following series of actions and encourages non-federal organizations to do the same. These recommendations address the identification, categorization, and prioritization of HVAs. They focus on an assessment approach to identify and prioritize risks and weaknesses for timely mitigation and architectural enhancements based on the assessment results.

Action 1: Establish an Organization-Wide HVA Governance Program

- Organizations should take a strategic, enterprise-wide view of cyber risk that unifies the effort to protect HVAs against evolving cyber threats. Organizations should establish an office, team, or other governance structure to enable the incorporation of HVA activities (e.g., assessment, remediation, incident response) into broader planning activities for information system security and privacy management, such as Enterprise Risk Management and Contingency Planning.

Action 2: Identify and Prioritize High Value Asset Information Systems

- The following categories are useful in identifying HVAs. Organizations can determine what information systems they have that fall into one or both of these categories:
  - Information Value - the data the system processes, stores, or transmits is of high value to the organization and/or adversaries; and
  - Mission Essential - the owning organization cannot accomplish its mission essential functions within the expected timeliness without this information system

Action 3: Consider the Interconnectivity and Dependencies of HVA Systems when Determining which Systems are HVAs

- For example, if the authentication solution for an HVA is the organization's centralized Active Directory solution then the Active Directory solution may also be considered an HVA due to critical dependency.
- Consider dependent and interdependent systems that can impact the operations of an HVA and its ability to perform a mission.
- Protect the dependent and interdependent systems at the same level as the primary systems.

Action 4: Develop a Methodology for Prioritizing HVAs Based on Criticality and Mission Importance

- A prioritized HVA list can be used by the organization to prioritize monitoring, assessment, and contingency actions across the organization's operational functions.
- Identify and prioritize the HVAs so that everyone in the organization understands the most important systems.
- Ensure that the most important systems receive the highest priority of support, funding, and operations to keep the mission going.

Action 5: Develop an Assessment Approach Based on HVA Prioritization

- Organizations should develop an assessment approach for their HVAs based on the prioritization. For example, an independent third-party contractor assesses the top 50% of the systems and the bottom 50% of the systems are self-assessed by internal staff. Organizations should determine the best approach for assessments based on their risk management appetite/tolerance.
- This should include implementing an HVA organizational risk assessment where all HVA systems receive assessments at least once every three years based on risk.
- Performing regular information security checks against these HVAs is critical in ensuring that the systems and information are protected at the appropriate levels commensurate with risk.

Action 6: Ensure Timely Remediation of Identified Vulnerabilities

- Organizations should make efforts to remediate any assessment risks/weaknesses within 30 days.
- If remediation cannot be completed within 30 days, a detailed remediation plan should be developed and tracked to completion.

HELPFUL LINKS AND REFERENCE MATERIALS

CISA Binding Operational Directive 18-02 - Securing High Value Assets:
https://cyber.dhs.gov/bod/18-02/
CISA Binding Operational Directive 16-01 - Securing High Value Assets (Revoked):
https:// cyber.dhs.gov/bod/16-01/
CISA, Securing High Value Assets:
https://www.dhs.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf
CISA, High Value Asset Control Overlay:
https://www.dhs.gov/sites/default/files/publications/HVA%20Control%20Overlay%20v1.0_0_0.pdf
The Office of Management and Budget (OMB), Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program:
https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
The Office of Management and Budget (OMB), Managing Information as a Strategic Resource:
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf