EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

December 10, 2018

M-19- 03

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mick Mulvaney
Director

SUBJECT: Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program

Purpose

This memorandum provides guidance on the enhancement of the High Value Asset (HVA) program operated by the Department of Homeland Security (DHS), in coordination with the Office of Management and Budget (OMB). It outlines expectations for the following areas:

- Establishing Enterprise HVA Governance;
- Improving the Designation of HVAs;
- Implementing Data-Driven HVA Prioritization;
- Increasing the Trustworthiness[1] of HVAs;
- Protecting Privacy and HVAs; and
- Defining HVA Reporting, Assessment, and Remediation Requirements.

This memorandum consolidates and updates previous requirements from OMB memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, and OMB memorandum M-17-09, *Management of Federal High Value Assets*, and rescinds these memoranda in accordance with burden reduction guidance in OMB memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memorandum*.

[1] Circular A-130 defines a 'Trustworthy information system' as an information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

Introduction

With the creation of the HVA initiative in 2015, the Federal Government's CFO Act agencies[2] took a pivotal step toward the identification of its most critical assets. DHS, in coordination with OMB, established a capability to assess agency HVAs, resulting in the identification of critical areas of weakness and plans to remediate those areas of weakness. With the dynamic adversarial threat to the security and resilience of HVAs, it is essential that the initiative evolve to take a more comprehensive view of the risk to the Federal enterprise and the measures available to mitigate those risks. As such, the HVA program is expanding to support all agencies, including both CFO Act and non-CFO Act agencies, in HVA identification, assessment, remediation, and response to incidents. As the HVA program[3] matures, the Federal Government will bolster its vigilant protection of HVAs and meet the objectives of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* to improve risk management across the executive branch.

Establishing Enterprise HVA Governance

The Federal Government requires agencies take a strategic, enterprise-wide view of cyber risk that unifies the effort to protect HVAs against evolving cyber threats. In execution of the HVA program, agencies shall:

1. Designate an integrated agency-level office, team, or other governance structure to enable the incorporation of HVA activities (*e.g.*, assessment, remediation, incident response) into broader agency planning activities for information system security and privacy management, such as Enterprise Risk Management, Capital Planning and Investment Control (CPIC), Contract Management, and Contingency Planning.[4]
    - Chief Operating Officers (COOs)[5] shall regularly coordinate with these governance structures and mission owners to ensure that HVA activities, including those directed by DHS, are executed in a timely manner.

[2] The CFO Act agencies include the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, the Treasury, Veterans Affairs, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Office of Personnel Management, Small Business Administration, Social Security Administration, U.S. Agency for International Development, and U.S. Nuclear Regulatory Commission. 31 U.S.C § 90l(b).

[3] The HVA program does not supersede, but rather compliments the responsibilities of agencies as required by the Federal Information Security Modernization Act of 2014, 44 U.S. Code § 3554.

[4] Contingency Planning refers to actions taken to mitigate risk to information systems as defined in Federal Information Processing Standards and their implementing guidance.

[5] Pursuant to M-18-19, the agency COO is responsible for providing overall organization management to improve and achieve the mission and goals of the agency. COOs provide organizational leadership to improve performance of both mission and management functions.

2. Establish, evaluate, and update (where appropriate) HVA information sharing agreements with OMB, DHS, and other agencies to promote cross-agency sharing, coordination, and cooperation. This includes, but is not limited, to the sharing of authorization packages[6] and other cybersecurity related information.

Improving the Designation of HVAs

This memorandum provides agencies with an updated approach to HVA identification, moving from a single definition[7] of what constitutes an HVA toward the establishment of multiple categories under which an agency may designate an HVA.[8] This approach allows agencies to have greater flexibility in the identification and designation of their most critical assets.

An agency may designate Federal information or a Federal information system as an HVA when it relates to one or more of the following categories:

- *Informational Value* – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
- *Mission Essential* – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.
- *Federal Civilian Enterprise Essential (FCEE)* – The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

While agencies are principally responsible for designating their HVAs, OMB and DHS may also designate HVAs at agencies based on potential impact to national security.

Implementing Data-Driven Prioritization

It is imperative that agency Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Financial Officers (CFOs), Senior Agency Officials for Privacy (SAOPs), or other roles, in coordination with OMB and DHS, work together to appropriately

[6] Pursuant to Circular A-130, an 'Authorization package' means the essential information that an authorizing official uses to determine whether to authorize the operation of an information system or the use of a designated set of common controls. At a minimum, the authorization package includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.'

[7] This approach replaces the definition of HVA in OMB Memorandum M-17-09.

[8] The HVA designation is not applicable to national security systems (NSS) as defined in 44 U.S.C. § 3552 (FISMA). Owners and operators of NSS, which includes those systems critical to the execution of military, intelligence, and cryptologic operations, shall follow all relevant Committee on National Security Systems (CNSS) issuances, as well as Department of Defense (DoD) and/or Intelligence Community (IC) guidance regarding the protection of sensitive information and systems with respect to NSS. If a situation arises whereby designating a system satisfies the conditions of both an NSS and HVA, the system shall be designated a NSS.

allocate agency resources for HVAs and to ensure the effective protection of HVAs. Through collaboration and data-driven prioritization, the executive branch can gain better visibility into which HVAs require ongoing visibility and support. In execution of the HVA program, agencies shall:

1. Adopt the methodology provided by DHS to prioritize their HVAs and associated HVA activities; and
2. Provide feedback to DHS to improve the output and usage of the methodology.

Increasing the Trustworthiness of HVAs

Increasing the trustworthiness of information systems is a significant undertaking that requires a substantial investment in the requirements, architecture, design, and development of systems, system components, applications, and networks. Agencies shall:

1. Implement the systems security engineering principles, concepts, techniques, and System Development / Engineering Lifecycle (SDLC / SELC) in NIST SP 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* for all HVAs;[9]
2. Ensure that security and privacy requirements for HVAs reflect the systems security engineering principles, concepts, and techniques that have been incorporated into their enterprise architecture and procurements; and,
3. Ensure that the procurement of information systems, system components, applications, or services designated as HVAs or that are intended to support HVAs, include requirements for developers, manufacturers, and vendors to employ systems security and privacy engineering concepts and methods, security and privacy design principles, secure coding techniques, and trusted computing methods in the system development life cycle.[10]

Protecting Privacy and HVAs

Federal law and policy establish requirements for the proper handling of PII. To both ensure compliance with those requirements and to manage privacy risks, SAOPs are required to review agency HVAs and identify those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. For each HVA identified in the SAOP's review, the SAOP shall ensure that all required privacy documentation and materials are complete, accurate, and up-to-date. This includes the information system's privacy plan[11] – a formal document that details the

[9] NIST SP 800-160, Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems is available at: http://csrc.nist.gov/publications.

[10] Appendices F and G in NIST Special Publication 800-160, provide guidance on *Design Principles for Security* and *Engineering and Security Fundamentals*.

[11] Pursuant to Circular A-130, the security plan and the privacy plan may be separate or integrated into one consolidated document.

privacy controls in place or planned for an information system or environment to meet applicable privacy requirements and manage privacy risks, how the controls have been implemented, and the methodologies and metrics used to assess the controls.

As part of the agency's privacy continuous monitoring program required by OMB Circular A-130,[12] SAOPs should ensure they have a reliable process in place to identify and assess on an ongoing basis any changes to HVAs that may impact the privacy and/or that may result in the need for additional or modified privacy documentation. This includes ensuring that privacy impact assessments[13] (PIAs) remain current and accurately reflect the information created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by the associated information technology.

Defining Reporting, Assessment, and Remediation Requirements

Reporting: Consistent with DHS Binding Operational Directives (BODs),[14] agencies shall report all of their designated HVAs to DHS. Although HVAs can be either classified or unclassified systems, agencies are only required to report their non-national security HVAs to DHS.

Assessment: All agencies are responsible for the ongoing authorization[15] of their information systems to ensure accuracy of information pertaining to the security and privacy posture of their HVAs. HVA assessments are critical to maintain an unbiased view of the risk associated with maintaining an HVA. In execution of the HVA program, agencies shall:

1. Consistent with DHS BODs, ensure HVA assessments are conducted at the frequency determined by DHS;

---

[12] Refer to OMB Circular No. A-130 located here: https://www.whitehouse.gov/omb/information-for-agencies/circulars/.

[13] Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under that section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

[14] Refer to https://cyber.dhs.gov/bod/ for more information on DHS BODs.

[15] Pursuant to Circular A-130, agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually. However, this general requirement to test and evaluate the effectiveness of information security and privacy policies, procedures, and practices does not imply that agencies must assess every selected and implemented security and privacy control at least annually. Rather, agencies must continuously monitor all implemented security and privacy controls (i.e., system-specific, hybrid, and common controls) with a frequency determined by the agency in accordance with the Information Security Continuous Monitoring (ISCM) and Privacy Continuous Monitoring (PCM) strategies.

- DHS, third-party assessor, or an agency's independent assessment entity[16] shall conduct the assessments, incorporating them as part of existing agency cybersecurity programs.
- For HVA assessments conducted by DHS, agencies shall engage and actively participate in the assessment process. Also, agencies shall establish and continuously maintain a Rules of Engagement (ROE) authorization with DHS to enable the timely assessment of HVAs.
- Any third-party or agency independent HVA assessments that are conducted in lieu of a DHS assessment must be conducted within the DHS defined frequency and follow DHS' assessment requirements. Accordingly, agencies shall establish a legally binding agreement with third-party and/or agency independent assessment entities that clearly establishes the roles and responsibilities amongst the parties, and incorporates DHS's government-wide baseline requirements for HVAs. These requirements shall form the basis of the HVA assessment.

2. Provide the results of all HVA assessments conducted by third-Party and/or agency independent assessment entities to DHS; and
3. Incorporate requirements into all existing and future contracts and service-level agreements (SLAs) that enable the execution of HVA assessments for Federal information systems,[17] including cloud-managed services and contractor-owned, contractor-operated systems.

Remediation: Agencies are responsible for developing prioritized remediation plans to address HVA assessment findings. Agencies are encouraged to coordinate these remediation plans with their CIO, CISO, CFO, Chief Acquisition Officer (CAO), and SAOP prior to finalization. In execution of the HVA program, agencies shall:

1. Within a year of transmitting assessment findings to DHS, develop plans to update the technology or architecture of those HVAs for which the corrective action is attributed to obsolete or unsupported technology, or critical deficiencies in the solution architecture;
    - Agencies shall submit these plans to their OMB Resource Management Offices (RMOs).
    - It is strongly recommended that the plans identify impediments in policy, resource allocation, workforce, or operations, and should maximize the use of shared IT services, application and data-level protections, and authorized cloud-based architectures (where applicable) to rectify the gaps.
2. Work with their budget offices and governance structures to ensure that potential remediation strategies are in alignment with the organization's broader cybersecurity risk-based budgeting plan outlined in OMB capital planning and cybersecurity budgeting guidance;[18]

[16] Independent assessment entities within an agency may perform an HVA assessment provided the entity reports to the CIO and the remaining C-Suite.

[17] Per Circular A-130, "Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

[18] Refer to Circular A-11 https://www.whitehouse.gov/omb/information-for-agencies/circulars/ and IT Budget – Capital Planning Guidance https://www.whitehouse.gov/omb/management/egov/

3. Provide all remediation plans to address HVA assessment findings to DHS, confirming that these plans conform to DHS reporting requirements; and
4. For any assessment findings that the agency determines it will not remediate or develop a plan to remediate, the agency shall provide a letter to OMB and DHS setting forth the reasoning and indicating the acceptance of risk. The agency head must sign the letter.

Government-wide Responsibilities

The following agencies serve in a government-wide capacity to improve the management and security of HVAs.

DHS is responsible for implementing the following actions:

1. Establishing processes to maintain visibility into the security and privacy posture of HVAs across the Federal Government;
2. Establishing measures of performance and measures of effectiveness to support continuous improvement of the HVA program;
3. Developing, maintaining, and disseminating, in coordination with OMB, a methodology for identifying and prioritizing HVAs that incorporates agency feedback (where appropriate);
4. Providing guidance to agencies concerning HVA reporting frequency, including the method for collection and data elements required;
5. Determining, in coordination with OMB, the baseline frequency by which an assessment is required for Federal HVAs;
6. Providing guidance to agencies on the process for reporting all HVA assessment results and remediation plans to DHS;
7. Providing guidance to agencies on sharing cybersecurity related information for HVAs;
8. Working with agencies, where possible, in bolstering protections for HVAs identified as having the greatest risk; and
9. Defining and maintaining requirements for HVA assessments that agencies can leverage when procuring assessment services outside of those provided through DHS or offered through GSA's Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) on IT Schedule 70 and its successor contract vehicle.

GSA is responsible for implementing the following actions:

1. Coordinating with DHS and OMB to align the HACS SIN with DHS requirements for HVA assessments, and include additional services that may be leveraged to improve the security of HVAs;
2. Incorporating feedback by OMB and DHS on the usage of HACS SIN into future HACS SIN improvements; and
3. Maintaining, in coordination with the FAR Council, OMB, and DHS, standardized language that agencies can reference when modifying their contracts and SLAs to enable HVA assessments.

Rescissions

The issuance of this memorandum rescinds the following:

1. M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government; and
2. M-17-09, Management of Federal High Value Assets.

Policy Assistance

Address all questions or inquiries on this memorandum to OMB's Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.

Address privacy-related matters to OMB's Office of Information and Regulatory Affairs (OIRA) Privacy Branch via email: privacy-oira@omb.eop.gov.