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

THE DIRECTOR

December 9, 2016

M-17-09

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Management of Federal High Value Assets

PURPOSE

This Memorandum contains general guidance for the planning, identification, categorization, prioritization, reporting, assessment, and remediation of Federal High Value Assets (HVAs), as well as the handling of information related to HVAs by the Federal Government. It also outlines the responsibilities of Executive Branch departments and agencies, including the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and General Services Administration (GSA). The HVA initiative outlined in this memorandum is an ongoing government-wide activity intended to evolve over time.

This memorandum is directed to Federal Executive Branch departments and agencies (hereinafter "agencies") but does not apply to national security systems. Owners of national security systems should follow relevant Department of Defense (DOD) and Intelligence Community (IC) guidance regarding the protection of sensitive information and systems with respect to national security systems.[1]

INTRODUCTION

Federal Government HVAs enable the government to conduct essential functions and operations, provide services to citizens, generate and disseminate information, and facilitate greater productivity and economic prosperity. Federal agencies have long taken measures to identify, categorize, and secure Information Technology (IT) assets whose confidentiality, integrity, and availability are essential to their ability to operate and execute their missions. In recent years, continued increases in computing power combined with declining computing and storage costs

[1] Recognizing that existing IC and DOD technical controls for sensitive IT assets may not sufficiently address policy and strategic impacts and other enterprise risks, agencies operating national security systems are encouraged to apply the principles of enterprise risk management contained in this memorandum and to familiarize themselves with and, as appropriate, adopt approaches herein to ensure that national security systems are assessed, prioritized, and protected based on a comprehensive assessment of risk that encompasses threat information; system interdependencies; broader impacts to multiple organizations or the whole-of-government; and policy, business, and strategic impacts that go beyond agency-specific IT or operations.

and increased network connectivity have expanded the government's capacity to store and process data in order to improve service delivery to the public. This rise in technology and interconnectivity also means that the Federal Government's critical networks, systems, and data are more exposed to cyber risks. The Federal Government must continue to evolve its approach to managing risks to these HVAs and instantiating a continuous review of all critical networks, systems, and data.

The Federal Government is committed to identifying and prioritizing HVAs, assessing the HVAs' security posture, and taking needed protective actions. OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, issued on October 30, 2015, and the President's *Cybersecurity National Action Plan (CNAP)*, issued on February 9, 2016, recognized that the heightened threat environment and an increasing number of incidents involving Federal IT assets requires such action in order to strengthen our cybersecurity posture.

DEFINITION[2]

"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.

THE CURRENT LANDSCAPE

Existing Federal risk management policies, guidance, and standards that direct agencies to identify IT assets, perform risk assessments, and address risks related to IT assets also apply to HVAs. For example:

- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, directs agencies to look at risk across all functions of the agency and highlights IT as a component of the portfolio view of risk.

- The overarching Federal information management policy, OMB Circular No. A-130, *Managing Information as a Strategic Resource*, requires agencies to manage Federal information throughout the information life cycle and directs agencies to provide protection for their information commensurate with the risk and potential harm resulting from its compromise. Additionally, OMB Circular A-130 states that agencies must identify IT assets and maintain an inventory of agency information resources, and it specifically directs each agency to maintain an inventory of its respective information

[2] This replaces the definition of HVA in OMB Memorandum M-16-04.

systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).

- OMB Memorandum M-13-13, *Open Data Policy—Managing Information as an Asset*, requires that agencies create and maintain an inventory of data assets via an enterprise data inventory.

Once an agency identifies its IT assets and creates the appropriate inventories, the agency has additional obligations, for example:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidelines for applying the Risk Management Framework to Federal information systems, to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, then directs agencies to categorize their information and information systems based on the potential impact to an organization should events occur which jeopardize the information and information systems of an organization. Initial security categorizations pursuant to such guidance will help determine the baseline security controls that an agency must implement to protect Federal information and information systems at the security impact level determined by the FIPS 199 categorization. The specific controls chosen will be drawn from NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and guided by NIST SP 800-60 Volume I Revision 1, *Guide for Mapping Types of Federal Information and Information Systems to Security Categories*, tailored according to an assessment of risk by the owning agency.

While this HVA initiative is compatible with and must leverage existing policies and guidelines regarding IT assets, such as those listed above, agencies must also consider their HVA risks from a strategic enterprise-wide perspective. As such, the agency HVA process described herein requires explicit consideration of the following factors:

- Agencies' assessment of risk should not be limited to IT and other technical considerations. HVA risk assessments should incorporate operational, business, mission, and continuity considerations. All key stakeholders of an agency, to include the Chief Financial Officer (CFO), Chief Acquisition Officer (CAO), Senior Agency Official for Privacy (SAOP), mission, business, and policy owners as well as the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) organizations, should be engaged in evaluating HVA risks.

- Agencies' assessment of risk should consider not just the risk that an HVA poses to the agency itself, but also the risk of interconnectivity and interdependencies leading to significant adverse impact on the functions, operations, and mission of other agencies.

Further, agencies' assessment of risk should include the risk of significant adverse impact on national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

- Agencies' assessment of risk to an HVA should be informed by an 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 owing to demonstrated adversary interest in agencies' actual, related, or similar assets.

- All agency-identified HVAs will be reviewed by DHS and OMB in order to prioritize HVAs for assessment and remediation activities across government.

- Based on the DHS and OMB reviews, a select number of HVAs will be subject to a standardized assessment with the potential for additional services as needed.

THE AGENCY HVA PROCESS

Agencies must take a strategic enterprise-wide view of risk that accounts for all critical business and mission functions when identifying HVAs. Agencies must also establish appropriate governance of HVA activities across the enterprise and should integrate HVA remediation activities into agency planning, programming, budgeting, and execution processes. These efforts must align with OMB policy, Federal law and regulations, Federal standards and guidelines, and agency policies, processes, and procedures.

Figure 1: Agency HVA Process Framework

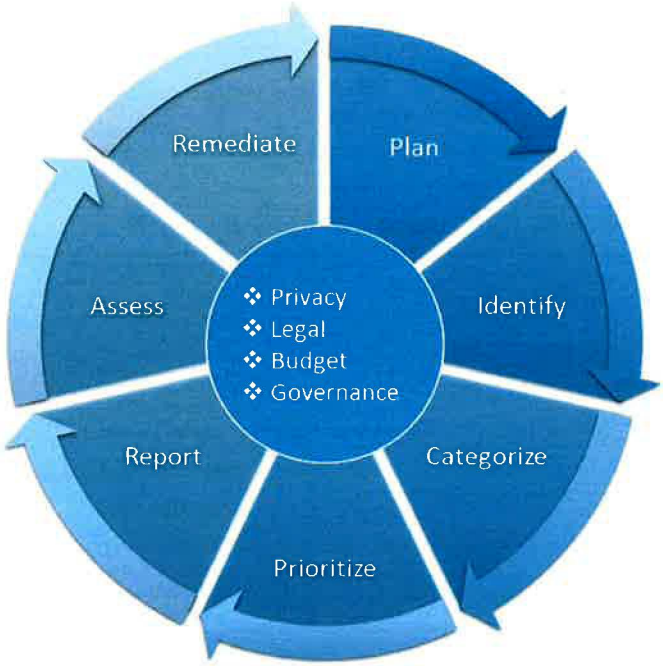

Figure one represents the continuous HVA process, including the specific actions that make up the process.[3]

PLAN:

Agencies must develop, maintain, and regularly update their HVA inventory lists, at least annually, to implement this guidance.[4] At a minimum, the planning process must include the following considerations:

- Stakeholder engagement, including identifying and engaging information system and information/data owners, business process experts, IT experts, information security experts, privacy experts, and risk management experts, as necessary;
- Review of business processes and identification of appropriate management controls to protect HVA and critical business functions over the entire data and information lifecycle;
- Governance and oversight, including identification of a senior accountable official and a lead office to be responsible to agency leaders and OMB for management of the overall HVA initiative;
- Engagement with third parties on behalf of the agency to ensure appropriate contract clauses or legal agreements are in place to assess and remediate system vulnerabilities as necessary;
- Engagement with contracting officers and the agency's general counsel to ensure all necessary agreements for contracted services, such as penetration testing, auditing, and security architecture reviews (SARs), are in place; and
- Incorporation of HVA activities into broader agency IT and information security and privacy management planning activities, including:
    - Enterprise risk management;
    - Budget, procurement, and contract management plans to address potential assessor findings;
    - Change management;

---

[3] **Plan**: Prepare for the HVA process, including stakeholder engagement, governance and oversight, third party engagement, and incorporation of HVA activities into broader agency IT planning.
Identify: Examine systems from the agency's perspective, adversary's perspective, and enterprise-wide perspective to determine those assets which may be considered HVAs.
Categorize: Organize information systems based on (among other things) system function, what kind of and how much information the system contains, the system's importance to the agency's mission, and the scale of impact from system loss or compromise.
Prioritize: Rank HVA systems in terms of risk, considering the categories of threat, vulnerability, and consequence.
Report: Agencies are responsible for keeping their internal HVA lists up-to-date. All CFO Act agencies are required to report their HVAs to DHS on an annual basis.
Assess: The HVA system(s) will be assessed by DHS through a Risk and Vulnerability Assessment (RVA), Security Architecture Review (SAR), and any additional services as deemed necessary.
Remediate: Agencies will receive a detailed report from DHS regarding the HVA system including recommended actions to address the findings.

[4] HVA management processes should take advantage of current security-related processes and artifacts produced by agencies in accordance with their responsibilities under FISMA, thus avoiding duplication and redundancies.

- Information Security Continuous Monitoring (ISCM) Strategy;
- IT lifecycle management, including plans to upgrade legacy components, system migration, and disposal;
- Privacy compliance and Privacy Continuous Monitoring (PCM);[5]
- Performance measurement and metrics; and
- Contingency planning.

IDENTIFY, CATEGORIZE AND PRIORITIZE:

Agencies should use the following guidelines to identify, categorize, and prioritize HVAs to ensure that information systems performing or enabling mission essential functions have been considered as potential HVAs and that appropriate agency stakeholders have been engaged.

- Start with an *agency-specific assessment* of risk by using FIPS 199[6] and NIST SP 800-60 to assist with information and information system identification and categorization.
- Next, consider the value of agency systems and data from a potential *adversary's perspective*. This means agencies should maintain awareness of malicious actor intent, capabilities, targeting, and trends based on government threat intelligence as well as commercial sources of threat intelligence. Such information includes cybersecurity threats to the agency by nation-state and criminal actors as well as current threat actor tactics, techniques, and procedures.
- Throughout the identification process, agencies should also take a *Federal enterprise-wide perspective* of the risks posed by their HVAs and of their mission responsibilities to both identify their most critical functions, information, and data and to use that information to categorize information systems as critical mission enablers or mission essential functions.
- Once an initial collection of HVAs has been identified, agencies should protect that collection according to the handling directions at the end of this guidance, take measures to determine the physical location of those HVAs, determine key stakeholders (including third parties) involved in the administration of those HVAs, clearly communicate roles and expectations to those stakeholders, and identify information system interdependencies.
- After the agency-level list of HVAs has been assembled, agency CIOs should ensure that the owners and operators of the HVAs are notified of their designation as an HVA.

Once the agency-level inventory of HVAs has been produced, agencies should develop a risk-based matrix of threats, vulnerabilities, impacts, and likelihood of compromise. The matrix should serve as a basis for prioritizing the agency's HVA assessment activities. This will support the delivery of an annual "Top 10" prioritized list of HVAs to OMB and DHS. For those HVAs that do not qualify as top 10, agencies have the discretion to rank and rate them using either a "1-to-n" or "tiered" approach.

[5] Per A-130, agencies are required to establish and maintain an agency-wide PCM program that implements the agency's PCM strategy

[6] There is no minimum FIPS categorization for a system to be considered an HVA, as FIPS ratings are only one factor to consider in the identification and prioritization process.

The following criteria should be used by agencies as additional inputs to their own prioritization when categorizing and prioritizing identified HVAs. This is not an exhaustive list, and it does not preclude agencies from considering additional criteria.

- Adversary and criminal interest;
- Nature and sensitivity of Federal information processed, stored, or otherwise utilized by the HVA;
- Whether the HVA contains Controlled Unclassified Information (CUI),[7] particularly one or more of the following:
    - PII on agency employees or customers;
    - CUI used for traveler/cargo vetting or other law enforcement purposes;
    - Proprietary information; and
    - CUI related to Federal or national critical infrastructure or key resources;
- Nature and sensitivity of processes controlled by the system, as in the case of an Industrial Control System (ICS) or Supervisory Control and Data Acquisition (SCADA) system;
- Quantity of information stored or handled by the HVA;
- Uniqueness of the stored or handled information or data and/or the information system function(s) (e.g., if the information system is a single point of failure);
- Degree to which the HVA is essential to supporting the agency's mission essential functions, including whether the HVA is connected with HVAs in other agencies so that a compromise could significantly impact mission essential functions within other agencies;
- Scale of impact (i.e., local, multiagency, Federal enterprise, national-level impact) of the loss or compromise of the information or data and/or information system functionality; and
- Nature of impact (i.e. national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people).

Many of these inputs focus on the potential resulting impact or consequence should the confidentiality, availability, or integrity of a given HVA be compromised. As agencies consider potential inputs for their own individual prioritization approaches, they should also consider privacy risk to individuals, potential threats to the HVA, as well as known vulnerabilities and the overall security posture of the HVA. All three categories of risk (threat, vulnerability, and consequence) should be considered when ranking HVAs.

[7] Per Executive Order (EO) 13556, *Controlled Unclassified Information*, Controlled Unclassified Information is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies, excluding information that is classified under EO 13526, *Classified National Security Information*, of December 29, 2009, or the Atomic Energy Act (P.L. 83-703), as amended.

REPORT:

All Federal agencies are responsible for keeping their internal HVA lists up-to-date. All CFO Act agencies[8] are required to report all of their HVAs, including the prioritized top 10 list, to DHS on an annual basis. DHS will coordinate with OMB and other interagency partners to ensure appropriate oversight and governance across the Federal Government. Although HVAs can be either classified or unclassified systems, agencies are only required to report their non-national security HVAs to DHS. **The Fiscal Year 2017 reporting date is January 15, 2017.** CFO Act agencies will be required to submit the following data fields to DHS on an INTELINK platform on either the Joint Worldwide Intelligence Communications System (JWICS) or Secret Internet Protocol Router (SIPR) platforms. Non-CFO Act agencies are encouraged, but not required, to follow the same review and reporting process. Agency HVA points of contact must maintain an active INTELINK account on either JWICS or SIPR. The required data fields are as follows:

- Agency Name;
- Agency Component or Bureau Name (if applicable);
- HVA Name;
- Is the HVA a Top 10 Priority HVA (yes/no);
- Description of HVA Function (maximum of 500 characters);
- Description of Impact of HVA Compromise to the Agency (maximum of 500 characters);
- Valid Authorization to Operate (ATO) (yes/no);
- Is the HVA an ICS or SCADA system (yes/no);
- Date of the Last HVA Assessment;
- Type of Assessor (Agency/DHS/Third-party);
- Current Plan of Action and Milestones (POA&M) to Remediate Assessment Findings (yes/no); and
- If Applicable, How Many Critical/High, Moderate, and Low Impact Actions Remain Incomplete from the Most Recent POA&M.

[8] Per 31 U.S.C § 901(b), as amended, the current 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, Environment 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.

ASSESS:

Pre-Assessment

In addition to the standard processes agencies must use for all information systems, to include tailoring security and privacy controls following the selection of the appropriate baseline (commensurate with NIST SP 800-53), agencies must prepare the HVA for assessment and ensure appropriate protections are in place by completing the steps listed below:

- **Implement and validate security controls** – Per the direction of Binding Operational Directive (BOD) 16-01,[9] and using the security engineering principles, concepts, and techniques in NIST SP 800-160, *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, agencies must implement the following security activities for all HVAs:
  - Secure configuration management;
  - Increased phishing awareness training and testing of personnel with access to HVAs;
  - Continual validation of strict access controls, including multifactor authentication;
  - Routine vulnerability scanning and remediation;
  - Increased monitoring and analysis of relevant audit logs;
  - Network segmentation;
  - Appropriate boundary protections;
  - Verification of data recovery capabilities;
  - Routinely tested incident response procedures; and
  - Maintenance of 100% automated asset visibility and control.
- **Identify system dependencies and interdependencies** – Agencies must identify the connections between HVAs and other systems, including other HVAs and non-HVAs, to understand critical dependencies.
- **Conduct security assessments of HVAs** – After validation of security controls and identification of dependencies and interdependences at the identified HVAs, the agency, in coordination with OMB and DHS, shall create and implement a plan for prioritizing and conducting assessments.
- **Ensure appropriate agreements with DHS or independent third-party assessment providers are in place to facilitate timely and comprehensive assessments** – All CFO Act agencies are required to participate in the HVA initiative and ensure all required legal agreements are signed and in place with DHS prior to commencement of assessment work.[10] This includes having a valid and signed standing Federal Network Authorization (FNA) and

[9] Published BODs are available to OMB MAX Executive Branch users at community.max.gov/x/RJQ5JQ.
[10] The ROE establish the guidelines and agreement between DHS and the agency, authorizing DHS, typically through DHS's National Cybersecurity Assessment and Technical Services (NCATS) to conduct RVAs on the agency's networks.

a Rules of Engagement (ROE) in place with DHS consistent with OMB M-16-03.[11] In addition, all Federal Executive Branch agencies are encouraged to follow these procedures.

All agencies are responsible for the ongoing assessment and authorization of their systems to ensure accuracy of information pertaining to the security posture of their HVAs. Agencies should leverage the results of security audits and voluntary third party assessments to ensure that HVAs are assessed on a regular basis. Following the assessments, DHS or, alternatively, an independent third party assessment organization will provide specific findings and recommendations and will work with agencies to develop a remediation plan to address findings discovered during the assessment. Agencies must ensure that the independent third party assessment findings and recommendations are provided to DHS in a timely manner. In addition to including appropriate confidentiality and data handling requirements in any agreements with independent third party assessors, agencies must ensure that relevant agreements with independent third party assessors specify that the agency is the sole owner of all agency information collected by the third party and such information and any derivative work, including notes and working documents, must be returned to the agency.

Assessment Process

HVA assessments will focus on the agency's assets, systems, information, data, and datasets as prioritized by the agency and will be reviewed by DHS in coordination with OMB. These assessments will not replace existing cybersecurity assessment programs for the agency. Agencies may work with DHS to receive comprehensive assessment services or may, and are encouraged to, procure similar HVA risk management services from commercial providers, so long as such services meet the DHS-established baseline requirements of the newly developed Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) on GSA's IT Schedule 70.[12]

HVA assessment activities include:

---

[11] OMB M-16-03 directed agencies (not only CFO Act agencies), consistent with applicable law, to provide a signed FNA to DHS by November 13, 2015, to ensure DHS, typically through US-CERT, can rapidly deploy on-site resources to conduct incident response activities, as necessary.

[12] The HACS SINS are comprised of the following cybersecurity services:
132-45A: Penetration Testing – Security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.
132-45B: Incident Response Services – These services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.
132-45C: Cyber Hunt Services – These activities are undertaken in response to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber hunt activities start with the premise that threat actors that are known to target some organizations in a specific industry, or organizations using specific systems, are likely to also target other organizations in the same industry or with the same systems. The processes use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks. Cyber hunt activities also include the investigation and analysis of all relevant response activities.
132-45D: Risk and Vulnerability Assessment – These activities include assessments of threats and vulnerabilities, deviations from acceptable configurations, and enterprise or local policy to assesses the current level of risk. The assessor then develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

- **Risk and Vulnerability Assessment (RVA)** – This service, provided by the DHS National Cybersecurity Assessment and Technical Services (NCATS) team, uses a number of techniques to identify weaknesses in the security posture of a given HVA. These can include network mapping, vulnerability scanning, phishing tests, wireless assessments, web application assessments, and database assessments.
- **Security Architecture Review (SAR)** – As appropriate and as resources are available, DHS will review the architecture of the HVA and develop recommendations for improving the security of the HVA related to the design and interconnections of the system. Once the SAR is complete, DHS will develop a report in collaboration with agency personnel to outline the current state of the agency's architecture and propose recommendations for a target state architecture. If requested by the agency, and if resources are available, DHS will also provide security engineering services to assist the agency with planning and implementation of the recommendations.
- **Additional Services, as needed** –
  - ICS / SCADA System Assessments – Comprised of tailored assessments based on the type of HVA, this assessment can supplement or replace other assessment activity, as appropriate.
  - Hunting for Potential Malicious Activity – A hunt capability can be deployed to search for malicious activity on any HVA and should be deployed, at a minimum, when the RVA or SAR finds evidence of a potential incident.
  - Federal Incident Response Evaluation – Based on the HVA and its inter-connectedness to other internal or external systems, including other HVAs, it may be appropriate to evaluate incident response readiness specifically tailored around the HVA or related systems.
- **Remediation Plans** – After the reviews of the HVA have been conducted, DHS, or the agency's independent third party assessment provider, will provide a report on the results, including detailed recommendations on actions that should be taken to address findings. Agencies will then be responsible for the creation of a remediation plan, to include a POA&M detailing specific actions, milestones, and timelines. The remediation plan does not represent the end of the process, as assessments should be completed on a continuous basis, and agencies should always ensure that HVAs receive an appropriate level of attention and resources to enhance their security posture.

***REMEDIATE*:**

The agency must complete its remediation plan expeditiously and should treat it as a priority. The remediation plan must include actions, milestones, and timelines for remediating the weaknesses or deficiencies identified in the assessment's findings. This plan should be validated by the CISO, CIO, CFO, SAOP (if the HVA contains PII), and CAO, and it should conform with DHS reporting requirements, including BOD 16-01 or any successor document for timely status updates.

Agencies should 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 the Capital Planning and Investment Control (CPIC) process.[13]

REVIEW PRIVACY COMPLIANCE AND PRIVACY RISK

Federal law and policy establish requirements for the proper handling of PII. To both ensure compliance with those requirements and 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, a formal document that details the 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. The plan also includes documentation required by the Privacy Act of 1974 (5 U.S.C. § 552a) (e.g., systems of records notices and Privacy Act Statements), the privacy provisions of the E-Government Act of 2002 (i.e., privacy impact assessments (PIAs)), Federal Information System Modernization Act of 2014 (FISMA), and relevant OMB guidance.

In addition, each agency's SAOP shall ensure that when PIAs are required for HVAs, they remain current and accurately reflect the information created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by the HVA. Further, these PIAs should be updated regularly to reflect any changes made to the information technology, agency practices, or HVAs that substantively alter the privacy risks associated with the use of such IT. The PIAs should appropriately document privacy risks and the controls required to mitigate those risks. Finally, SAOPs should ensure they have a reliable process in place to identify and assess on an ongoing basis any changes to the HVAs that may impact privacy risk and/or that may result in the need for additional or modified privacy documentation as part of the agency's PCM program and PCM strategy as required by OMB Circular No. A-130.

HANDLING INSTRUCTIONS

Handling guidance for agencies on information about HVAs can be found on MAX[14]

As noted throughout the document, the HVA initiative relies on the identification and prioritization of HVAs for testing and assessment based on numerous factors including the type and amount of information, criticality to mission essential functions, and adversary Tactics Techniques, and Procedures (TTPs). The identification and prioritization of these systems is critical to conducting assessments efficiently, but the results of these efforts are also an attractive target to anyone with malicious intent. To ensure the access needed to perform their appropriate functions while protecting the information about these critical systems, both agencies and

[13] www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy18_it_budget_guidance.pdf

[14] https://community.max.gov/x/Vg8_Rg - This handling guidance will be periodically updated depending on the outcomes of the HVA assessments or changes in TTPs.

independent third party assessors are expected to follow the handling guidance, except for classified national security information which should follow established guidance.

If a specific process or information is not listed, then it does not have unique handling or protection guidance in terms of being related to an HVA. However, any information submitted by outside agencies that is covered by separate classification guidance should retain the appropriate level of classification.

CONCLUSION

Risk management remains critical to the way the Federal Government protects its information, systems, and assets and improves its overall security posture. The HVA initiative enhances existing risk management processes by instituting a continuous process of planning, identification, categorization, prioritization, reporting, assessment, and remediation. Implementing this process will enable agencies to better understand the specific security needs of their most critical assets while gaining new insight as to how those assets fit into the larger Federal enterprise. Through a continuous review of all critical assets, systems, information, and data, civilian agencies can achieve a better understanding of what is on their network, what is valuable to their stakeholders, and what is valuable to individuals with malicious intent.

Going forward, agencies, DHS, OMB, and other stakeholders will continue to refine this process as lessons are learned and the threat landscape evolves. Agencies should integrate information gained from HVA efforts into their broader IT modernization work, budget discussions, mission delivery activities, and security initiatives to reduce duplication and ensure that all parts of the agency are aligned in prioritization and remediation activities.

Points of Contact:

Questions for OMB may be directed to ombcyber@omb.eop.gov

Appendix A: OMB, DHS, and GSA Roles and Responsibilities

This Appendix describes third party responsibilities for implementing OMB Memorandum M-17-XX, Management of Federal High Value Assets.

DHS or Independent Third Party Assessor:

- Work with the agency to ensure appropriate ROE documentation and other relevant legal agreements are in place.
- Ensure all access rights and entrance-on-duty requirements have been clearly established and communicated to the agency in order to ensure an efficient assessment.
- Conduct assessment(s) of HVAs in accordance with the signed ROE or other relevant legal agreement(s).
- Provide the assessed agency with a report outlining findings and recommendations.
    - Recommend to the assessed agency a prioritization of activities to appropriately remediate the findings of the assessment.
- In the case of DHS assessments, coordinate with OMB on the tracking of agency progress against the remediation plan.
- Develop future phases of the Continuous Diagnostics and Mitigation Program to address common capability and tool gaps discovered during the HVA assessment process.

OMB:

- Assist DHS with metrics and measurements for the HVA program as a government-wide initiative.
- Coordinate with DHS, the CIO Council, the CISO Council, the Cyber Interagency Policy Committee (Cyber-IPC), and other stakeholders as necessary to develop appropriate assessment tiers to ensure assessment teams are not delayed in focusing on the highest priority assessments.
- Monitor progress against the remediation plan through existing methods such as the CyberStat process and governance bodies such as the President's Management Council.
- Incorporate lessons learned from agency HVA assessments into future policy development.
- Work with agencies on budget formulation and execution related to HVA remediation.

GSA:

- Finalize and ensure the HACS SINs are kept up-to-date with multiple options for agencies to procure assessment services in a timely fashion.
- Provide agencies with options to procure remediation assistance.

Appendix B: HVA Requirements Tracker

This Appendix documents specific action items including deadlines and action item owners. OMB and DHS engagement with agencies will occur as needed to close out the action items.

Action		Deadline	Who is responsible?
Identify agency senior accountable officials and lead office to manage HVA processes and report to DHS.		January 15, 2017	All CFO Act agencies (all agencies encouraged)
Provide a "Top 10" prioritized list of HVAs to DHS (ref. "Report" section for required data fields).		January 15, 2017	All CFO Act agencies (all agencies encouraged)
Ensure agency HVA points of contact have active INTELINK accounts (JWICS or SIPR).		Annual, prior to "Top 10" HVA list submission	All CFO Act agencies (all agencies encouraged)
SAOP will ensure required privacy documentation, including any PIAs, are complete, accurate, and up-to-date for all HVAs that involve PII.		Immediate	All CFO Act agencies (all agencies encouraged)
Conduct HVA Pre-Assessments (ref. Assess: Pre-Assessment section for details)	Ensure implementation and validation of appropriate security controls for all HVAs.	Prior to HVA assessments	All CFO Act agencies (all agencies encouraged)
	Identify system dependencies and interdependencies.		
	Create and implement plan for conducting HVA assessments.		
	Establish required legal agreements, including valid FNAs and ROEs with DHS.		All CFO Act agencies (all agencies encouraged); DHS or other assessor
Establish and communicate access rights and entrance on duty requirements to agency.		Prior to HVA assessments	DHS or other assessor

Action		Deadline	Who is responsible?
Conduct HVA Assessments (ref. Assess: Assessment Process section for details)	Conduct RVAs through DHS NCATS or commercial provider.	Ongoing	All CFO Act agencies (all agencies encouraged); DHS or other assessor
	Conduct SAR.		
	(As needed) Conduct ICS assessments, hunting for malicious activity, and incident response evaluation.		
	Create remediation POA&M.		
Remediate HVA weaknesses and deficiencies	Provide agencies with detailed reports of assessments and prioritized recommendations and milestones for remediation.	Within 30 days of completion of assessment	DHS or other assessor
	Mitigate high-priority vulnerabilities (ref. BOD 16-01).	Within 30 days of receipt of assessment findings report	All CFO Act agencies (all agencies encouraged)
	Report status of high-priority vulnerabilities to DHS (ref. BOD 16-01).	Within 30 days of receipt of assessment findings report; every 30 days until all high-priority vulnerabilities are mitigated	All CFO Act agencies (all agencies encouraged)
Coordinate with OMB for tracking of agency progress in remediation.		Ongoing	DHS or other assessor
Provide agencies with government-wide vehicles to procure remediation assistance.		Ongoing	GSA