Secretary

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Binding Operational Directive *BOD-16-01*

Original Release Date:

Applies to: *All Civilian Chief Financial Officer Act Departments and Agencies*

FROM: Jeh Charles Johnson
Secretary

CC: Shaun Donovan
Office of Management and Budget

SUBJECT: **Securing High Value Assets**

A binding operational directive is a compulsory direction to federal, executive branch, civilian departments and agencies ("agencies") for purposes of safeguarding federal information and information systems. The Department of Homeland Security develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014. Federal agencies are required to comply with these DHS-developed directives.[1]

Background: Across the federal government, agencies operate high value assets that contain sensitive information or support critical government services. The President's Cybersecurity National Action Plan directs all agencies to improve the security of their high value assets. DHS will help agencies identify vulnerabilities in their high value assets and implement targeted security measures to mitigate those vulnerabilities.[2]

Required Actions: Agencies receiving this Binding Operational Directive shall take the following two actions:

---

[1] *See* 44 U.S.C. §§ 3552(b)(1), 3553(b)(2), 3554(a)(1)(B)(ii).

[2] This Binding Operational Directive aligns with and furthers the execution of the Office of Management and Budget's Cybersecurity Sprint Implementation Plan (CSIP), as restated in OMB *Memorandum 16-03*, which required agencies to "[i]mmediately identify agency specific [high value assets] and assess the security protections around those high value assets."

Action One – Identify and Submit a Lead Point of Contact

- Identify a lead point of contact who will be responsible for coordinating the agency's high value asset assessments with DHS.[3]
- Submit the name, email address(es), and phone number of your agency's lead point of contact as identified above to FNR.BOD@hq.dhs.gov within seven days from the issuance of this binding operational directive.
    - Submission of the same information for at least one backup point of contact encouraged.

Action Two – Participate in Assessment, Mitigation, and Remediation Activities

- Sign a DHS-provided rules of engagement document authorizing DHS to conduct risk and vulnerability assessments on agency high value assets. [4]
- Prior to an assessment authorized by the rules of engagement, begin to implement the mitigation measures listed in Appendix A for agency high value assets.
- Participate in the high value asset assessments authorized by the rules of engagement.
- If requested by DHS, participate in a security architecture assessment for select high value assets.
- Mitigate the high-priority vulnerabilities identified by DHS in the high value asset final assessment report within 30 days of receipt of the report or determine that mitigation is not feasible within that timeframe.
- Report the status of each high-priority vulnerability to the DHS email address below within 30 days of receiving the high value asset final assessment report. The status report must state that the vulnerability has been mitigated or explain the constraints preventing mitigation within 30 days and the steps that the agency is implementing to progress toward mitigation.
- Provide additional status updates every 30 days until all high-priority vulnerabilities have been addressed.

Progress Tracking: If an agency does not comply with the requirements of this Binding Operational Directive, DHS will follow up with each Deputy Secretary or equivalent, as appropriate.

DHS Point of Contact: Binding Operational Directive Team, FNR.BOD@hq.dhs.gov.

---

[3] To ensure that the designated point of contact is able to exchange necessary information with DHS, the individual should have appropriate clearances.

[4] DHS will identify to each agency the high value assets to be assessed under this Binding Operational Directive.

Appendix A: High Value Asset Mitigation Measures

Agencies are required to implement the following security activities at each high value asset identified for assessment by DHS.[5] DHS will validate whether these activities and any related protections have been appropriately implemented during each high value asset assessment and will provide the agency with a report on the extent of sufficient implementation.

1) **Ensure Secure Configuration Management**
   - High value assets must adhere to secure configuration settings as defined by the United States Government Configuration Baseline.[6]
     - If there is a mission need to deviate from the configuration baseline, that change must be documented and a mitigating control applied.
     - Any such documentation and mitigation must be approved by the Agency CIO or appropriately designated official.
2) **Increase/Enhance Phishing Awareness Training and Testing**
   - Agencies must conduct a phishing test on personnel with privileged access to high value assets prior to the DHS assessment.
3) **Implement Strict Access Controls**

   Agencies must:
   - limit the number of personnel with privileged access to high value assets.
   - limit user privileges to those necessary for the performance of job duties so that users have role-based access to only the information and resources that are necessary for a legitimate purpose.
   - ensure that all users with privileged access to high value assets are required to use multi-factor authentication for that privileged access.
   - ensure that all privileged-user activities with high value assets are tracked and logged to detect misuse and to help reduce the risk from insider threats or the risk posed by malicious actors using stolen credentials.
4) **Perform Routine Vulnerability Scanning and Remediation**
   - Agencies must perform credentialed vulnerability scans of high value assets to identify and rapidly patch security vulnerabilities.

---

[5] When agencies implement these activities, DHS's assessment can focus on more complex technical issues that will maximize the utility of the assessments.

[6] *See* http://usgcb.nist.gov/usgcb_content.html

- These scans are intended to identify significant vulnerabilities that require immediate remediation.

5) Improve Network Segmentation

- Agencies must limit network connections to and from high value assets and validate those connections using appropriate boundary defense and access control protections.