Homeland Security

Binding Operational Directive *BOD-15-01*

Original Release Date: *May 21, 2015*

Applies to: *All Federal Civilian Executive Branch Departments and Agencies*

FROM: Jeh Charles Johnson
Secretary of Homeland Security

CC: Shaun Donovan, Director
Office of Management and Budget

SUBJECT: **Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems**

A Binding Operational Directive is a compulsory direction to federal agencies regarding federal information security. The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives, and federal agencies are required to comply with the DHS-developed directives. See 44 U.S.C. §§ 3552(b)(1), 3553(b)(2), 3554(a)(1)(B)(ii) (Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283).

Background: Increasing cybersecurity risks are forcing organizations to focus more attention on information security. By identifying and mitigating vulnerabilities in the information technology (IT) environment, organizations can reduce the risk of attackers penetrating their networks and stealing information.

In accordance with Office of Management and Budget (OMB) Memorandum 15-01: *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, the Department's National Cybersecurity and Communications Integration Center (NCCIC) conducts persistent network and vulnerability scans of Federal Civilian Executive Branch Departments' and Agencies' ("Department and Agency") Internet-accessible systems to identify known vulnerabilities and configuration errors. As a result of this activity, reports are generated and delivered weekly, titled "Cyber Hygiene report," tailored for each Department and Agency, to

provide an enhanced understanding of the Department or Agencies' cyber posture, and to promote a secure and resilient IT infrastructure. The weekly reports illustrate the vulnerabilities detected, identify the affected systems, and provide mitigation guidance. Often times, the vulnerabilities identified through these scans are rated "critical."

Critical vulnerabilities with a Common Vulnerability Scoring System (CVSS) rating of "ten" on a scale of one to ten are included in each weekly "Cyber Hygiene report." CVSS is a vulnerability scoring system designed to provide a universally open and standardized method for rating IT vulnerabilities utilized by both government and private sector entities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal, and environmental properties of a vulnerability.

Critical vulnerabilities are typically remotely exploitable, have a low complexity to execute, utilize default or no authentication and impact confidentiality, integrity and availability. By their very nature, critical vulnerabilities detected through scanning are exposed to anyone with an Internet connection, are at imminent risk of exploitation by a malicious third party and should be immediately addressed.

The NCCIC has observed traffic targeting known vulnerabilities (e.g. Heartbleed) through the National Cybersecurity Protection System and recorded numerous incident reports across all critical infrastructure sectors where the root cause of compromise stemmed from outdated operating systems and applications (e.g. content management systems) and weak (to include instances of default) credentials. In addition, the NCCIC is aware that sophisticated advanced persistent threat actors have exploited several of these critical vulnerabilities in cyber incidents affecting Department and Agency networks, private sector, and state, local, tribal, and territorial entities.

In the future, the NCCIC scanning capability will benefit from the continued implementation of the Departments' Continuous Diagnostics and Mitigation (CDM) solutions across the Department and Agencies' IT infrastructure. This will allow for more robust information sharing of critical vulnerabilities (both Internet-exposed and internal) and assist the NCCIC in focusing Department and Agency assessments.

Required Actions:

All Departments and Agencies shall review and mitigate the critical vulnerabilities on their Internet facing systems identified by the NCCIC within 30 days of issuance of their weekly "Cyber Hygiene report." The timeliness of this mitigation is imperative given that all the vulnerabilities identified through a scan are Internet-accessible.

This Binding Operational Directive applies to all current and future critical vulnerabilities identified in the weekly "Cyber Hygiene report." Department or Agencies that are unable to mitigate a vulnerability within thirty days will provide a detailed justification to DHS outlining any barriers, planned steps for resolution, and a timeframe for mitigation. DHS,

through its Federal Network Resilience Division, will work directly with the Department or Agency to attempt to assist or address any constraints limiting expedited resolution of the vulnerability.[1]

Progress Tracking:

Beginning on the date of issuance of this Binding Operational Directive, all critical vulnerabilities identified on a Department or Agencies' weekly "Cyber Hygiene report" must be mitigated within 30 days of the initial reporting of a critical vulnerability:

- The NCCIC will leverage the weekly scans to track each Department and Agencies' progress mitigating its critical vulnerabilities.

- DHS will provide quarterly "Cyber Hygiene report" updates to OMB to ensure Department and Agency results are synchronized with OMB cybersecurity oversight initiatives.

- Mitigated vulnerabilities will automatically be detected and removed from future reports.

- Any vulnerability that cannot be mitigated within thirty days must be reported to DHS with a detailed justification explaining the constraints limiting expedited mitigation and the steps that the Department or Agency is implementing to progress toward mitigation.

Point of Contact:

National Cybersecurity Assessment & Technical Services (NCATS) Program
Email: ncats@hq.dhs.gov

[1] See 44 U.S.C. § 3553(b)(2)(C) & 3.