




BINDING OPERATIONAL DIRECTIVE

Binding Operational Directive 19-02 (*BOD 19-02*)

Original Release Date: *April 29, 2019*

Applies to: *All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence*

FROM: Christopher C. Krebs 
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CC: Russell T. Vought
Director (Acting), Office of Management and Budget

SUBJECT: **Vulnerability Remediation Requirements for Internet-Accessible Systems**

A binding operational directive is a compulsory direction to federal, executive branch, departments and agencies for purposes of safeguarding federal information and information systems. 44 U.S.C. § 3552(b)(1). Section 3553(b)(2) of title 44, U.S. Code, authorizes the Secretary of the Department of Homeland Security (DHS) to develop and oversee the implementation of binding operational directives. Federal agencies are required to comply with these directives. Id. § 3554(a)(1)(B)(ii). These directives do not apply to statutorily defined "national security systems" or to systems operated by the Department of Defense or the Intelligence Community. Id. § 3553(b), (d), (e)(2), (e)(3).

Background:

As federal agencies continue to expand their Internet presence through increased deployment of Internet-accessible systems, and operate interconnected and complex systems, it is more critical than ever for federal agencies to rapidly remediate vulnerabilities that otherwise could allow malicious actors to compromise federal networks through exploitable, externally-facing systems. Recent reports from government and industry partners indicate that the average time between discovery and exploitation of a vulnerability is decreasing as today's adversaries are more skilled, persistent, and able to exploit known vulnerabilities. The federal government must continue to take deliberate steps to reduce the overall attack surface and minimize the risk of unauthorized access to federal information systems as soon as possible.

Binding Operational Directive 15-01: *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*¹ established requirements for federal agencies to review and remediate critical vulnerabilities on Internet-facing systems identified by the National Cybersecurity and Communications Integration Center (NCCIC) within 30 days of issuance of their weekly Cyber Hygiene report. Since its issuance in 2015, the prior National Protection and Programs Directorate and the current Cybersecurity and Infrastructure Security Agency (CISA) oversaw a substantial decrease in the number of critical vulnerabilities over 30 calendar days and a significant improvement in how agency teams identified and responded to these vulnerabilities in a timely manner. By implementing specific remediation actions, and initiating ongoing monitoring and transparent reporting via CISA's Cyber Hygiene service,² BOD 15-01 helped drive progress and enhance the federal government's security posture. In support of BOD implementation, CISA leverages Cyber Hygiene scanning results to identify cross-government trends and persistent constraints, and works with the Office of Management and Budget (OMB) to help impacted agencies overcome technical and resource challenges that prevent the rapid remediation of vulnerabilities.

The federal government must continue to enhance our security posture, reduce risks posed by vulnerable Internet-accessible systems, and build upon the success of BOD 15-01 by advancing federal requirements for high and critical vulnerability remediation to further reduce the attack surface and risk to federal agency information systems.

Revocation:

This directive supersedes BOD 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems* (May 21, 2015), which is hereby revoked.

Required Actions:

To ensure effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning, federal agencies shall complete the following actions:

1) Ensure Access and Verify Scope

- a) Ensure Cyber Hygiene scanning access by removing Cyber Hygiene source IP addresses from block lists.
- b) Within five working days of the change, notify CISA at NCATS@hq.dhs.gov of any modifications to your agency's Internet-accessible IP addresses. This includes newly acquired Internet-accessible IP addresses or re-assigned Internet-accessible IP addresses that are no longer part of the agency's asset inventory.
- c) Upon request from CISA, submit updated Cyber Hygiene agreements to NCATS@hq.dhs.gov.

2) Review and Remediate Critical and High Vulnerabilities

¹ DHS Binding Operational Directive 15-01 was issued on May 21, 2015.

² Cyber Hygiene leverages the Common Vulnerability Scoring System (CVSS), which is a vulnerability scoring system designed to provide a universally open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize vulnerability management strategies by providing a score representative of the base, temporal, and environmental properties of a vulnerability.

- a) Review Cyber Hygiene reports issued by CISA and remediate the critical and high vulnerabilities detected on the agency's Internet-accessible systems as follows:
- Critical vulnerabilities must be remediated within 15 calendar days of initial detection.
 - High vulnerabilities must be remediated within 30 calendar days of initial detection.
- b) If vulnerabilities are not remediated within the specified timeframes, CISA will send a partially populated remediation plan identifying all overdue, in-scope vulnerabilities to the agency POCs for validation and population. Agencies shall return the completed remediation plan within three working days of receipt to FNR.BOD@hq.dhs.gov. The recipient of the remediation plan shall complete the following fields in the remediation plan:
- (1) Vulnerability remediation constraints
 - (2) Interim mitigation actions to overcome constraints
 - (3) Estimated completion date to remediate the vulnerability

Progress Tracking:

CISA will monitor federal agency progress and will engage agency senior leadership, such as Chief Information Security Officer (CISO), Chief Information Officer (CIO), and Senior Accountable Official for Risk Management (SAORM), as necessary and appropriate, when the agency has not met the Required Action deadlines specified above.

CISA also will track the remediation of critical and high vulnerabilities through persistent Cyber Hygiene scanning and will validate compliance with the BOD requirements through these reports.

CISA Actions:

- CISA will provide regular reports to federal agencies on Cyber Hygiene scanning results and current status, and a Federal Enterprise 'scorecard' report to agency leadership.
- CISA will provide standard remediation plan templates for federal agencies to populate if remediation efforts exceed required timeframes.
- CISA will engage agency POCs to discuss agency status and provide technical expertise and guidance for the remediation of specific vulnerabilities, as requested and appropriate.
- CISA will engage Agency CIOs, CISOs, and SAORMs throughout the escalation process, if necessary.
- CISA will provide monthly Cyber Hygiene reports to OMB to identify cross-agency trends, persistent challenges, and facilitate potential policy and/or budget-related actions and remedies. The report will also ensure alignment with other OMB-led cybersecurity oversight initiatives.

CISA Points of Contact:

- General Inquiries and Reporting: FNR.BOD@hq.dhs.gov
- Technical Inquires: NCATS@hq.dhs.gov