Secretary

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

Homeland Security

Binding Operational Directive *BOD-16-02*

Original Release Date: September 27, 2016

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

FROM: Jeh Charles Johnson
Secretary

CC: Shaun Donovan
Director, Office of Management and Budget

SUBJECT: **Threat to Network Infrastructure Devices**

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 (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). Federal agencies are required to comply with these DHS-developed directives.[1]

Background: For several years, network infrastructure devices have been the attack-vector of choice for sophisticated hackers and advanced threat actors. The DHS/National Cybersecurity and Communications Integration Center (NCCIC) expects this trend to continue. Network infrastructure devices are the devices that transport the communications required for the data, applications, services, and multimedia that your agencies rely upon each and every day to fulfill their mission. As the security of desktop and laptop computers and servers have improved, based on our collective efforts to improve federal cybersecurity, our adversaries are adjusting their tactics, techniques, and procedures and have begun targeting network infrastructure devices.

Three particularly urgent issues require immediate attention across all impacted Federal agencies: hacking tools targeting firewalls, Cisco Adaptive Security Appliance, and Cisco ROM Monitor Integrity. If not addressed, impacts may include denial-of-service attacks, data theft, and the altering of data, all of which can be accomplished much more effectively and in a more subtle and targeted manner from compromised

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

network infrastructure, and can impede workforce productivity and the ability to execute your agency's mission.

We have witnessed our adversaries attempting to take advantage of these vulnerabilities to exploit Federal agency networks. We anticipate that our adversaries will continue to try to take advantage of these vulnerabilities, as well as vulnerabilities we have yet to identify. To help combat this exigent threat, and to adapt to the threat environment your agencies' should expect to face moving forward, my Department has provided a series of mitigation steps and best practices to ensure your agency is as protected as possible. The NCCIC has published an Analysis Report AR-16-20173 and associated Technical Annexes, which addresses all three of these issues. The NCCIC has also deployed signatures in the EINSTEIN system to detect suspicious activity related to these exploitation tools and vulnerabilities, to help protect the Federal civilian executive branch. The NCCIC will continue to analyze information for additional mitigation steps to protect our Federal networks and will develop Technical Annexes in the future under this directive as necessary.

Regardless of their generic common vulnerability score, the vulnerabilities identified in AR-16-20173 and associated Technical Annexes are now deemed critical for purposes of Binding Operational Directive 15-01 (issued May 2015). When these vulnerabilities are found on external-facing systems they will also be flagged in each agency's BOD 15-01 scorecard report.

Required Actions:

- Perform all actions in the "Solution" sections of the "Technical Annexes" to the NCCIC Analysis Report AR-16-20173 no later than 45 days after issuance of this Directive.[2]
- Report to DHS, through the OMB MAX Connect Portal, either full mitigation or provide a detailed plan of action and milestones explaining the constraints preventing mitigation and the associated compensating controls established no later than 45 days after issuance of this Directive.
- Provide additional reports or plans of action and milestones every 30 days thereafter until full mitigation is achieved.

Progress Tracking: If an agency does not comply with the requirements of this 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.

Attachment: NCCIC Analysis Report AR-16-20173 and associated Technical Annexes

[2] Agencies must comply with the deadline timeframe referenced in the "Required Actions" of this directive for any future Technical Annexes of NCCIC Analysis Report AR-16-20173, triggered on the date of issuance of each additional Technical Annex.