Secretary

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

Homeland Security

October 17, 2016

Binding Operational Directive *BOD-16-03*

Original Release Date:

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: **2016 Agency Cybersecurity Reporting Requirements**

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: Providing a comprehensive framework for ensuring the effectiveness of information security controls over federal information and information systems requires centralized reporting of agency information security incidents and the general information security posture of agencies. Accordingly, FISMA requires agencies to report security incidents to the DHS Federal information security incident center.[2] The United States Computer Emergency Readiness Team (US-CERT), part of DHS's National Cybersecurity and Communications Integration Center (NCCIC), serves as the Federal information security incident center. FISMA further requires agencies to provide annual reports to the Office of Management and Budget (OMB), DHS, and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.[3] FISMA itself specifies some of the requirements of these reports,[4] and also requires DHS to issue Binding Operational Directives specifying additional requirements for those reports.[5] This directive satisfies those requirements.

---

[1] *See* 44 U.S.C. §§ 3552(b)(1), 3553(b)(2), 3554(a)(1)(B)(ii).
[2] *Ibid.* § 3554(b)(7)(c)(ii).
[3] *Ibid.* § 3554(c)(1)(A).
[4] *Ibid.*
[5] *Ibid.* § 3553(b)(2)(A-B).

FISMA Reporting Requirements: All agencies shall comply with the following requirements.

Requirements for Reporting Security Incidents to DHS:

- Report security incidents to US-CERT in accordance with the current guidelines found at https://www.us-cert.gov/incident-notification-guidelines which are updated as necessary.

Requirements for the 2016 Annual FISMA Reports:

- Agency Fiscal Year 2016 Annual FISMA Reports shall include the Chief Information Officer (CIO), Inspector General (IG), and Senior Agency Official for Privacy (SAOP) metric information detailed in the annual FISMA metrics located here: https://www.dhs.gov/publication/fy16-fisma-documents. This requires no additional action from federal agencies beyond the requirements stated in the OMB Memorandum on *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements.*
- By November 10, 2016, the CIO, IG, and SAOP metrics shall be submitted to OMB and DHS via CyberScope.

Requirements in Preparation for the 2017 Annual FISMA Reports:

- Agencies shall view the FY 2017 Annual FISMA CIO metrics available at *https://www.dhs.gov/publication/fy17-fisma-documents* and plan accordingly so they can include these metrics in their FY 2017 FISMA Reports.

Progress Tracking: DHS will track submission of the reports required above and follow up with OMB or the relevant agency to address non-compliance as appropriate.

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