EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2013

M-14-04

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Sylvia M. Burwell
Director

SUBJECT: Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

The attached memorandum provides instructions for meeting your agency's Fiscal Year (FY) 2013 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). It also includes reporting instructions on your agency's privacy management program.

The Office of Management and Budget (OMB) identified cybersecurity as one of 14 Cross Agency Priority (CAP) Goals for FY 2013 and FY 2014, which were established in accordance with the Government Performance and Results Modernization Act to build on the statutory requirements provided for in FISMA. The CAP goals are available at http://goals.performance.gov/. The cybersecurity CAP goals, which build upon work from prior years, are helping agencies improve cybersecurity performance by focusing efforts on what data and information are entering and exiting their networks, who is on their systems, and what components are on their information networks as well as when their security status changes. To accomplish these goals the Administration is prioritizing: (1) measuring agency implementation of Trusted Internet Connections; (2) focusing on strong authentication through the use of multi-factor authentication in accordance with Homeland Security Presidential Directive-12; and (3) performing monitoring of security controls in federal information systems and environments in which those systems operate on a continuous basis. The FY 2013 FISMA metrics issued by the Department of Homeland Security established minimum and target levels of performance for these priorities, as well as metrics for other key performance areas.

As discussed in OMB Memorandum 10-28, *"Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),"* DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543. As stated in previous FISMA guidance issued by OMB, agencies are required to adhere to Department of Homeland Security (DHS) direction to report data through CyberScope. Additionally, OMB requires that the head of each agency submit, as part of the agency's annual report, a signed electronic copy of an official letter to CyberScope providing a comprehensive overview reflecting his or her assessment of the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA for the agency.

I ask for your help in overseeing your agency's implementation of the reporting guidance outlined in the attachments.

Questions for OMB may be directed to Carol Bales at 202-395-9915 or fisma@omb.eop.gov. Questions regarding FISMA metrics and Cyberscope reporting may be directed to the Cybersecurity Performance Management Office, Federal Network Security Branch, DHS, at FISMA.FNS@dhs.gov or (703) 235-5045.

Attachments

Attachment: Fiscal Year (FY) 2013 FISMA Reporting Guidance

The FY 2013 FISMA metrics are classified into three categories as follows:

Administration Priorities (AP)	The AP metrics highlight three areas: Trusted Internet Connection (TIC) capabilities and utilization, mandatory authentication with Personal Identity Verification (PIV), and Continuous Monitoring.
Key FISMA Metrics (KFM)	Key metrics are the additional metrics outside of the Administration priorities that are measured (scored).
Baseline (BASE)	Baseline FISMA metrics are not scored, but used to establish current baselines against which future performance may be measured.

The FY 2013 FISMA metrics are located on the Department of Homeland Security (DHS) website at: http://www.dhs.gov/federal-network-resilience

Required Action

To comply, agencies will carry out the following activities:

- **Submit monthly data feeds.** The Chief Information Officers (CIO) of CIO Council member agencies will submit monthly data feeds through CyberScope. Agencies must load data from their automated security management tools into CyberScope on a monthly basis for a limited number of data elements. For more information, refer to the Frequently Asked Questions related to data feeds.[1]

- **Respond to security posture questions on a quarterly/annual basis.** In addition to providing the data feeds described above, agency CIOs, Inspectors General, and Senior Agency Officials for Privacy are also required to answer a set of information security questions in CyberScope. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness. The CIOs of CIO Council member agencies report on a quarterly basis, and Inspectors General and Senior Agency Officials for Privacy report on an annual basis.

DHS will continue to provide agencies with the status of their current cybersecurity posture, based on CyberScope data, and ask agencies to complete a Plan of Action for improving specific cybersecurity capabilities. Agencies will provide quarterly and FY targets and demonstrate progress toward those targets as they mature their programs.

- **Participate in CyberStat accountability sessions and agency interviews.** Equipped with the reporting results from CyberScope and agency Plans of Action, DHS, along with the Office of Management and Budget (OMB) and the White House National Security Staff, will continue to conduct CyberStat reviews of selected agencies. CyberStat reviews are face-to-face, evidence-based meetings to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing focused strategies for improving information security posture.

DHS will continue the annual interviews with agencies' CIO and Chief Information Security Officers (CISO) based on their agency's security posture. Each interview session has three distinct goals:
- Assessing progress towards the administration cybersecurity priorities and other FISMA compliance and challenges.
- Identifying security best practices and raising awareness of FISMA reporting requirements.
- Establishing meaningful dialogue with the agency's senior leadership.

The information collected in these interviews will also inform OMB's annual FISMA Report to Congress.

---

[1] Frequently asked questions related to data feeds can be found on the CyberScope information page within the OMB MAX Portal. The URL for the page is https://max.omb.gov/community/display/Egov/Data+Feeds.

- **Submit Privacy documents.** As part of the annual report, Senior Agency Officials for Privacy are to submit the following documents through CyberScope:

- Description of the agency's privacy training for employees and contractors
- Breach notification policy
- Progress update on eliminating unnecessary use of Social Security Numbers
- Progress update on the review and reduction of holdings of personally identifiable information.

OMB is requiring agencies to submit these four documents whether or not the documents have changed from versions submitted in previous years.

Reporting deadlines

Monthly Data Feeds:	Agencies are required to submit information security data to CyberScope by close of business on the 5th of each month. Small and micro agencies are not required to submit monthly reports, although they are highly encouraged to do so.
Quarterly Reporting:	CIO Council agencies are expected to submit metrics data for first, second and third quarters. For first quarter, agencies must submit their updates to CyberScope between January 1-15. For second quarter, agencies must submit their updates to CyberScope between April 1-15. For third quarter, agencies must submit their updates to CyberScope between July 1-15. Agencies are not expected to submit metrics data for the fourth quarter, other than what is required for the annual report.
Annual Report:	The due date for all agencies to submit their annual FY 2013 FISMA report through CyberScope is December 2, 2013.

Additional Requirements

- Agencies shall review their performance of the administration's FISMA cybersecurity priorities with their Performance Improvement Officer, as these priorities will receive additional emphasis in FY 2014 as the Administration reports agency progress towards the cybersecurity Cross Agency Priority (CAP) goals. The cybersecurity CAP goals consist of the following activities: Continuous Monitoring; Trusted Internet Connections (TIC) capabilities and traffic consolidation; and strong authentication using HSPD-12 Personal Identity Verification (PIV) cards for logical access.

- Agencies should note that a PIV card, compliant with Homeland Security Presidential Directive (HSPD) 12, is required for access to CyberScope. FISMA submissions will not be accepted outside of CyberScope. For information related to CyberScope, please visit: https://max.omb.gov/community/display/Egov/CyberScope+Documentation

- As part of the annual report, agencies are also asked to submit an electronic copy of an official letter to CyberScope, signed by the head of the agency, providing a comprehensive overview reflecting his or her assessment of the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA for the agency.

Points of Contact

Please direct questions regarding FISMA to the Cybersecurity Performance Management Office, Federal Network Security Branch, DHS, at FISMA.FNS@dhs.gov or (703) 235-5045.

For OMB policy related questions, please contact Carol Bales, (202) 395-9915 or fisma@omb.eop.gov.