Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

FISM 14-01

FEDERAL INFORMATION SECURITY MEMORANDUM

FOR: Heads of Executive Departments and Agencies

FROM: Andy Ozment
Assistant Secretary
Office of Cybersecurity and Communications

SUBJECT: Fiscal Year 2014 Metrics for the Federal Information Security Management Act of 2002 and Agency Privacy Management Act and Operational Reporting Instructions

Purpose

The purpose of this memorandum is to provide the metrics and operational reporting instructions for the Fiscal Year (FY) 2014 reporting periods under the Federal Information Security Management Act of 2002[1] (FISMA).

FY 2014 FISMA Reporting Guidance

The FY 2014 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 2014 FISMA metrics are located on the 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.** Chief Information Officers (CIO) will submit monthly data feeds through CyberScope. Agencies must load data from their automated security management tools into CyberScope on a monthly basis for Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposure (CVE) data elements. For more information, refer to the Frequently Asked Questions related to data feeds.

[1] Title III, Pub. L. No. 107-347

- **Respond to security posture questions on a quarterly/annual basis.** In addition to providing the data feeds described above, agency CIO, Inspectors General (IG), and Senior Agency Officials for Privacy (SAOP) 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 measures of effectiveness. The CIOs report on a quarterly basis, SAOP and IG 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 fiscal year 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 CAP Goal Action Plan, DHS, along with the Office of Management and Budget (OMB) and the White House National Security Council (NSC), 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, measurable outcomes, for improving information security posture.

  DHS will continue the annual interviews with agencies' CIO and Chief Information Security Officer (CISO) based on their agency's security posture. Each interview session has four 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;
  - Better understanding how DHS can support the D/A's security efforts; and
  - Establishing meaningful dialogue with the agency's senior leadership.

  Information collected in these interviews will also inform OMB's annual *Report to Congress on the Implementation of the Federal Information Security Management Act of 2002.*[2]

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:	In FY2014, agencies will be expected to submit metrics data for the second and third quarters. 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:	To meet the OMB draft annual report submission suspense, agencies must submit annual FY2014 reports in CyberScope no later than Friday, November 14th, 2014.

[2] http://www.whitehouse.gov/omb/e-gov/docs

Additional Requirements

- 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, the head of the agency should submit 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 agency-specific information security policies, procedures, and practices, and compliance with the requirements of FISMA.

- As part of the annual report, Senior Agency Officials for Privacy are to submit the following documents through CyberScope as directed in M-14-04:

    - 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 (PII).

Authorities

- *Federal Information Security Management Act*, Title III of the E-Government Act of 2002 (Pub. L. No. 107-347).

- M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010.

- M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013.

Points of Contact

Please direct questions regarding FISMA to Cybersecurity Performance Management (CPM), Federal Network Resilience, DHS, at FNR.FISMA@HQ.DHS.GOV.

cc: Director, Office of Management and Budget