U.S. Department of Homeland Security
Arlington, VA 22203

Homeland Security

February 15, 2012

FISM 12-02

FEDERAL INFORMATION SECURITY MEMORANDUM

FOR: Heads of Executive Departments and Agencies

FROM: Greg Schaffer
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate

SUBJECT: FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

Purpose

The purpose of this memorandum is to introduce updates and provide reporting instructions regarding the Federal Information Security Management Act (FISMA) program for Fiscal Year 2012 (FY12).

Background

Federal Departments and Agencies (D/As) must remain vigilant to defend their information systems, especially in a resource-constrained environment, balancing system security with operational capability through a risk management process. Many threats can be mitigated by following established cybersecurity best practices, but advanced attackers start with the weakest vulnerabilities, and then escalate in sophistication. The FY12 FISMA metrics build upon the baseline established in FY10 and FY11, and increase in sophistication to mitigate more advanced attackers.

Prior FISMA metrics documents (Chief Information Officer (CIO) & Inspector General (IG)) solely contained metric questions. New in FY12, the Department of Homeland Security (DHS) instituted norms and best practices to ease FISMA reporting. DHS also included specific definitions of terms and explanations as to why questions are being asked. This clarifies and provides uniformity of specific terms and interpretation of results. These changes were based on requests and suggestions received from various D/As and the Federal CIO Council Information Security and Identity Management Committee (ISIMC).

In addition, the FY12 metrics highlight Administration FISMA cybersecurity priorities, which are based on Federal government mandates and the most cost-effective Federal-wide security controls D/As can use to enhance the security of their information systems. These priorities focus on addressing the basic challenges of what is entering and exiting, who is on and what is on D/A networks.

Specific Updates for FY12 CIO Metrics

All metrics are classified into three categories: Administration Priorities (AP), Key FISMA Metrics (KFM), and Baseline (BASE). The AP metrics highlight three areas: Trusted Internet Connection (TIC) capabilities and utilization, mandatory authentication with Personal Identity Verification (PIV), and Continuous Monitoring. Key metrics are the additional metrics outside of the Administration

priorities that are measured (scored). Baseline FISMA metrics are not scored, but used to establish current baselines against which future performance may be measured.

Specific Updates for FY12 Inspectors General Metrics

One of the major changes initiated for FY12 IG Metrics is to include a one-to-one mapping of the CIO Metrics Control Areas, allowing the IGs to report the maturity of the control areas on which the CIOs report. This was introduced to ensure the IGs move towards measuring maturity of the control area rather than simply measuring an agency's compliance. The questions asked of the IGs in these areas have been raised from more tactical compliance questions to strategic risk management questions.

Additionally, all the changes under FY12 CIO Metrics (stated above) related to Guidance, Definition, and Purpose and Use have been incorporated into the FY12 IG Metrics.

From a structure and format perspective, previous years' IG Metrics were organized into three sections (a, b, and c). These sections equated to a response of either Yes, Maybe, or No. A majority of the responses reported by D/As were "Maybe". Hence the decision was made to remove sections (a, b, and c) and focus more on ascertaining maturity; as most D/As reported they were somewhat compliant in all of the Control Areas.

Required Action

To comply, D/As will carry out the following activities:

- **Submit monthly data feeds to CyberScope.** CyberScope is the platform for the FISMA reporting process. Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy as well as micro agencies will all report through CyberScope. D/As must load data from their automated security management tools into CyberScope on a monthly basis for a limited number of data elements. These reporting requirements will mature over time as DHS, in collaboration with the D/As, evolve and additional metrics and capabilities are developed.

  DHS will provide advance notice to D/As as these metrics evolve. The initial monthly reporting metrics and schema for FY12 will remain identical to the metrics and schema used for the autofeed portion of the FY 2011 reporting cycle. Revisions of metrics will be published in CyberScope and on the CyberScope page within the Office of Management and Budget (OMB) MAX Portal prior to the reporting period in order to allow sufficient time for adoption. As associated data feed schemas are revised, they will be posted on the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) web page as well as the CyberScope page within the OMB MAX Portal.[1]

- **Respond to security posture questions.** In addition to providing the data feeds described above, D/As 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.
- **Participate in CyberStat accountability sessions and agency interviews.** DHS will provide D/As with the status of their current cybersecurity posture, based on CyberScope data, and ask

[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.

D/As to complete a Plan of Action for improving specific cybersecurity capabilities. D/As will provide maturity targets to demonstrate quarterly and fiscal year targets in working towards implementation maturity through FY 13.

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 conduct CyberStat reviews of selected D/As. CyberStat reviews are face-to-face, evidence-based meetings to ensure D/As are accountable for their cybersecurity posture, while at the same time assisting them in developing focused strategies for improving information security posture.

DHS will interview D/A's CIO and CISO on their agency's security posture. Each interview session shall have three distinct goals:

- Assessing the agency's 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 the FY12 FISMA Report to Congress.

Effective Dates of Compliance

- Monthly Data Feeds: D/As are required to submit information security data to CyberScope by close of business on the 5th calendar day of each month. Small and micro D/As are not required to submit monthly reports, although they are highly encouraged to do so.
- Quarterly Reporting: D/As will be expected to submit metrics data for second and third quarters. For second quarter, D/As must submit their updates to CyberScope between April 1-15, 2012. For third quarter, D/As must submit their updates to CyberScope between July 1- 15, 2012. D/As are not expected to submit metrics data for the first and fourth quarters, other than what is required for the annual report.
- Annual Reporting: The due date for annual FY12 FISMA reporting through CyberScope is November 15, 2012.

Additional Requirements

- D/As 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

- Consistent with prior years' guidance, the D/A head should submit an 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 D/A.

- Senior Agency Officials for Privacy are to submit the following documents through CyberScope:
  - Breach notification policy if it has changed significantly since last year's report
  - Progress update on eliminating unnecessary use of Social Security Numbers
  - Progress update on the review and reduction of holdings of personally identifiable information.

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.

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

cc: Director, Office of Management and Budget

Attachment: FY 2012 FISMA CIO Metrics