



**Homeland  
Security**

September 4, 2013

FISM 13-01

**FEDERAL INFORMATION SECURITY MEMORANDUM**

FOR: Heads of Executive Departments and Agencies

FROM:  Roberta G. Stempfley  
Acting Assistant Secretary  
Office of Cybersecurity and Communications

SUBJECT: FY 2013 Metrics for the Federal Information Security Management Act 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) 2013 reporting periods under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347).

**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 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 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.

- 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 Agency Head 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 information security policies, procedures, and practices, and compliance with the requirements of FISMA for the agency.

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

- 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.

#### **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 Resilience Branch, DHS, at [FISMA.FNS@dhs.gov](mailto:FISMA.FNS@dhs.gov) or (703) 235-5045.

cc: Director, Office of Management and Budget