



August 24, 2011

FISM 11-01

FEDERAL INFORMATION SECURITY MEMORANDUM FOR THE HEADS OF
EXECUTIVE BRANCH CIVILIAN DEPARTMENTS AND AGENCIES

FROM:  Roberta G. Stempfley, Acting Assistant Secretary, Office of Cybersecurity & Communications, Department of Homeland Security

SUBJECT: Announcing Trusted Internet Connections (TIC) Reference Architecture v2.0

This Federal Information Security Memorandum (FISM)¹ informs the heads of executive branch civilian departments and agencies of the revised TIC Reference Architecture v2.0.

The TIC Reference Architecture v2.0 introduces new, and clarifies existing, mandatory critical capabilities. In addition to mandatory critical capabilities, the TIC Reference Architecture v2.0 includes recommended capabilities based on evolving technologies and threats. Recommended capabilities are considered desirable, but do not have well-defined standards due to evolving technologies, threats, or requirements. TIC Access Providers (TICAPs) and Managed Trusted Internet Protocol Service (MTIPS) providers should plan for recommended TIC capabilities, and implement them as federal and industry standards are more fully defined. In the next revision of the TIC Reference Architecture, these recommended capabilities are expected to become mandatory critical capabilities.

The TIC Reference Architecture v2.0 and additional information is available on the OMB MAX Portal (requires a .GOV or .MIL e-mail address to register):

<https://max.omb.gov/community/display/Egov/Trusted+Internet+Connections>

The TIC Reference Architecture v2.0 applies to:

- agencies designated as TICAPs;
- commercial carriers designated as MTIPS providers; and
- all federal executive branch civilian agencies procuring Networkx MTIPS or using TICAP services.

Agencies are reminded they still must complete the following previously established TIC Reference Architecture v1.0 Milestones.

Previous TIC v1.0 Milestones:

January 1, 2011. Approved TICAP departments and agencies and Networkx MTIPS providers will schedule their next TIC Compliance Validation (TCV)/Cybersecurity Compliance Validation

¹ The Department of Homeland Security issues Federal Information Security Memoranda to inform federal departments and agencies of their responsibilities, required actions, and effective dates to achieve federal information security policies.

(CCV) annual assessments with the Department of Homeland Security's Federal Network Security Branch, Compliance & Assurance Program.

January 31, 2011. All other executive branch civilian departments and agencies route all external connections, including to the Internet, through a TIC v1.0-compliant TICAP or MTIPS provider.

Individual Dates. Approved TICAP departments and agencies achieve 100% technical capabilities and 100% consolidation of external connections, including those to the Internet, according to their individual TIC Plans of Actions & Milestones (POA&Ms) submitted to the TIC Program Office.

DHS issues this memorandum pursuant to the following authorities:

- The Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541-3549,
- Office of Management and Budget's (OMB) M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and DHS* (assigning to DHS certain responsibilities under FISMA), and
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, *Comprehensive National Cybersecurity Initiative* (especially paragraphs 15 and 25).

Additional relevant documents include:

- OMB M-08-05: *Implementation of Trusted Internet Connections (TIC)*
- OMB M-08-16: *Guidance for Trusted Internet Connection Statement of Capability (SOC) Form*
- OMB M-08-27: *Guidance for Trusted Internet Connection (TIC) Compliance*
- OMB M-09-32: *Update on the Trusted Internet Connections Initiative*

For additional information or questions, please contact Sean Donelan, TIC Program Management Office, Federal Network Security Branch, Department of Homeland Security at tic@dhs.gov or by telephone 703-235-5122.



August 24, 2011

FISM 11-02

FEDERAL INFORMATION SECURITY MEMORANDUM FOR THE HEADS OF
EXECUTIVE DEPARTMENTS AND AGENCIES

FROM:  Roberta Stempfley, Acting Assistant Secretary, Office of Cybersecurity and
Communications, Department of Homeland Security

SUBJECT: FY 2011 Reporting Instructions for the Federal Information Security Management Act
and Agency Privacy Management

This Federal Information Security Memorandum (FISM)¹ provides instructions for meeting your agency's FY 2011 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). It also includes reporting instructions for your agency's privacy management program.

The goal for Federal information security in FY 2011 is to build a defensible Federal enterprise that enables agencies to harness technological innovation, while protecting agency information and information systems. To maximize the timeliness and fidelity of security-related information, the collection of data should be a by-product of existing continuous monitoring processes, not a bolt-on activity that redirects valuable resources from important mission activities. As stated in previous FISMA guidance, agencies are required to adhere to Department of Homeland Security (DHS) direction to report data through CyberScope. This shift from the once-a-year FISMA reporting process to a monthly reporting of key metrics through CyberScope allows security practitioners to make decisions using more information – delivered more quickly than ever before.

Agency Reporting Activities

To comply with this guidance, agencies will carry out the following activities:

1. Establish monthly data feeds to CyberScope;
2. Respond to security posture questions; and
3. Participate in CyberStat accountability sessions and agency interviews

1. Monthly Data Feeds

Effective next month, agencies must load data from their automated security management tools into CyberScope on a monthly basis for a limited number of data elements. While full implementation of automated security management tools across agencies will take time, agencies should report what they can using output from their automated security management tools. These reporting requirements will mature over time as the efforts of the Chief Information Officer (CIO) Council's Continuous Monitoring Working Group (CMWG), in collaboration with the agencies, evolve and additional metrics and capabilities are developed.

¹ The Department of Homeland Security issues Federal Information Security Memoranda to inform federal departments and agencies of their responsibilities, required actions, and effective dates to achieve federal information security policies.

DHS will provide advance notice to agencies as these metrics evolve. The initial monthly reporting metrics and schema for FY 2011 will remain identical to the metrics and schema used for the auto-feed portion of the FY 2010 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 NIST Security Content Automation Protocol (SCAP) web page as well as the CyberScope page within the OMB MAX Portal.

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/x/EqQrFQ>

2. Information Security Questions

In addition to providing the data feeds described above, agencies 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.

3. CyberStat Review Sessions and Agency Interviews

Building on the TechStat model, DHS launched CyberStat accountability sessions in January 2011. Through CyberStat, DHS cybersecurity experts engage with selected agencies to help them develop focused actions plans for improving their information security posture. CyberStat is grounded in analysis that is based on data provided through CyberScope and other key data sources. The development of clear and consistent metrics for CyberScope has improved the ability of agencies to have more accountability for outcomes. As DHS works with agencies to improve data quality, the insights provided through CyberStat and CyberScope will enable DHS to assist agencies in quickly addressing problems that pose risks.

DHS-led CyberStat sessions promote accountability and assist Federal civilian agencies in driving progress with key strategic enterprise cybersecurity capabilities. Specifically, CyberStat is designed to:

- Highlight capability areas where agencies must place additional focus;
- Help agencies remove roadblocks to meeting requirement standards; and
- Recognize agencies in those areas where they are meeting requirement standards.

CyberStat sessions feature representatives from DHS, OMB, the National Security Staff (NSS), and agency teams working together to carefully examine program data with a focus on problem solving. The outcome is a prioritized action plan for the agency to improve overall agency performance. Information compiled from the review process will also give DHS, OMB, NSS and other relevant stakeholders a holistic viewpoint of the cybersecurity posture of the Executive Branch of the Federal Government, informing future policy and oversight decisions.

A team of government security specialists will interview agencies not selected for a formal CyberStat review. These interviews will be focused on specific threats that each agency faces as a consequence of its unique mission.

Effective Dates of Compliance

- **Monthly Data Feeds:** Agencies are required to submit information security data to CyberScope by close of business on the fifth calendar day of each month. Small and micro agencies are not required to submit monthly reports, although they are highly encouraged to do so.
- **Quarterly Reporting:** Moving forward, agencies will be expected to submit metrics data for 2nd and 3rd quarters. For 2nd quarter, agencies must submit their updates to Cyberscope between April 1st and April 15th. For 3rd quarter, agencies must submit their updates to CyberScope between July 1st and July 15th. Agencies are not expected to submit metrics data for 1st or 4th quarters, other than what is required for the annual report.
- **Annual Reporting:** The due date for annual FISMA reporting through CyberScope is November 15, 2011.

Additional Requirements

- CyberScope is the platform for the FISMA reporting process. Agencies should note that a Personal Identity Verification card, compliant with Homeland Security Presidential Directive 12, is required for access to CyberScope. No FISMA submissions will be accepted outside of CyberScope. For information related to CyberScope, please visit: <https://max.omb.gov/community/x/EgQrFQ>
- CIOs, Inspectors General, and Senior Agency Officials for Privacy will all report through CyberScope. Micro agencies will also report using this automated collection tool.
- Consistent with prior years' guidance, the agency 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 agency.
- 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; and
 - Progress update on the review and reduction of holdings of personally identifiable information.

Please direct questions on 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.

Attachment: FY 2011 Frequently Asked Questions on Reporting for FISMA

cc: Director, Office of Management and Budget