February 2014

INFORMATION SECURITY

Evaluation of FTC's Information Security Program and Practices for Fiscal Year 2013

What We Found

The IG's independent FISMA evaluation for FY 2013 determined that the FTC is in substantial compliance with applicable security and privacy requirements.

The IG's CyberScope FISMA metrics submission to the Department of Homeland Security showed that FTC information assets are reasonably protected against threats originating from within and outside the agency, but there are opportunities for improvement. These include process changes to Information Technology (IT) governance practices and continued maturation of the FTC security and privacy programs.

FTC information security and privacy programs are maturing through self-initiated actions and improvements initiated in response to IG recommendations:

- Documentation is revised and standardized as part of ongoing operations and maintenance activities;
- Enterprise-level oversight practices are improving as newly instituted IT governance boards begin to influence IT planning and resource allocation; and
- Security and privacy processes are revised to accommodate changes in governmentwide requirements.

The foundation for a National Institute of Standards and Technology risk-based model was laid in FY 2012 and continues to evolve; however continued improvement of the FTC information security and privacy programs requires consistent application of information security and privacy policies.

What We Recommend

Program consistency and compliance needs to be reinforced through visible monitoring and oversight by FTC IT governance boards and senior management.

Why We Did This Study

The Federal Information Security Management Act of 2002 (FISMA) provides a comprehensive framework for ensuring the effectiveness of technical, administrative, and physical security controls over Federal information resources. FISMA requires an annual Inspector General evaluation of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines and an assessment of the level of security afforded to associated information assets.

The evaluations provide agency senior management and others with the information needed to determine the effectiveness of overall security programs, ensure the confidentiality and integrity of data entrusted to the FTC, and to develop strategies/best practices for cost effectively improving information security.

The FTC Office of Inspector General contracted with Allied Technology Group, Inc. to conduct an evaluation to determine the status of the FTC's information and privacy programs at September 30, 2013, as required under FISMA and associated guidance. A full report on our evaluation was prepared for FTC internal use only.