INFORMATION SECURITY

Evaluation of FTC's Information Security Program and Practices for Fiscal Year 2014

What We Found

As summarized in the FISMA reporting metrics submitted through CyberScope and in our full evaluation report, the OIG independent evaluation determined that the FTC information security and privacy programs provide reasonable assurance that FTC information assets are adequately protected, but there are opportunities for improvement.

The opportunities for improvement include process changes to resolve identified areas of concern and continuation of the maturation of the FTC security and privacy programs.

In the latter part of FY 2011, FTC established the basis for mature risk-based information security and privacy programs by issuing its *Information Technology Governance Program Charter*. FTC governance practices have been improving as it becomes increasingly embedded into FTC planning activities.

However, the increasing rate of change demonstrated the need for continued emphasis on implementing the mature processes that include the structures and artifacts necessary to ensure and document that adequate security and privacy is maintained as the IT environment evolves. This increased focus will help FTC continue to modernize and improve its security and privacy programs as it addresses mission changes and new threats and initiatives to resolve identified vulnerabilities.

What We Recommend

Successful evolution of the FTC information assurance and privacy programs will require continued senior management attention to ensure

1. Continuing to evolve FTC governance practices and expand the use of CPIC and investment analysis.
2. Acceleration of FTC's implementation of NIST SP 800-39 compliant risk-based governance and IT investment processes.
3. Completion of an appropriate configuration management plan and ensuring that it is effectively applied to the FTC and across all FTC systems.
4. Revision of FTC's process for determining minor applications and documenting security controls.
5. Applying its revised governance process to PIV implementation.
6. Development of a disaster recovery strategy and implementation plan.

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 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 independent evaluation to determine the status of the FTC's information and privacy programs at September 30, 2014 as required under FISMA and associated guidance.