Report In Brief

EVALUATION OF FTC's PROGRAM AND PRACTICE

December 2011

INFORMATION SECURITY

Fiscal Year 2011

AR 12-002

Why We Did This Study

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the Federal Trade Commission (FTC), to develop, document, and implement an agency-wide information security program. FISMA also requires each Inspector General (IG) to conduct an annual independent evaluation of its agency's information security program and practices.

The Office of Inspector General (OIG) contracted with Allied Technology Group, Inc. (Allied Technology) to perform the FY 2011 IG FISMA evaluation of the FTC information assurance and privacy programs.

The objective was to provide an evaluation of the effectiveness of the FTC information assurance and privacy programs and compliance with OMB and National Institute of Standards and Technology (NIST) guidance. This is a public version of a sensitive report that we issued in December 2011.

What We Recommend

To improve FTC security and privacy programs and bring them current with OMB and NIST guidance, we recommended improvements in the areas of risk management, capital planning, and information security continuous monitoring program.

What We Found

The evaluation showed that the FTC has established an information security program that is in substantial compliance with applicable security and privacy requirements.

In FY 2010, the FTC security efforts were hampered by deficient performance resulting from the conversion of its infrastructure support to a performance-based contract. In FY 2011, the FTC Office of the Chief Information Officer (OCIO) executed a special effort to mitigate the infrastructure concerns. This effort required the OCIO staff to perform much of the security-related infrastructure work that had been included in the support contract and at the same time continue to advance the FTC information assurance program. The OCIO effort was largely successful in mitigating immediate security vulnerabilities and establishing the foundation for a successful, cost effective information assurance program.

The FTC Information Security Program is documented in a number of policies and procedures that define a program structure compliant with FISMA requirements. The OCIO has an ongoing effort to ensure that FTC policies and procedures remain current with governmentwide guidance and is developing a multi-volume document (*The Federal Trade Commission Information Security Program Handbook*) that consolidates FTC security practices. The modernized environment includes increased acquisition of application services under a performance-based contracting approach. The FTC is also exploring opportunities to securely move FTC business applications into commercial "clouds," an approach that is intended to reduce costs while increasing the capability to scale services to fluctuating requirements

The FTC increased the coordination of its information assurance and privacy programs through its Privacy Steering Committee (PSC) in FY 2011. The increased coordination recognizes that information assurance and privacy requirements must be fully integrated to successfully protect FTC information assets.

The status of the FTC information assurance and privacy programs were summarized in the DHS FISMA reporting metrics submitted through Cyberscope. As stated in the Cyberscope metric report, the IG independent evaluation of the FTC information assurance and privacy programs resulted in a determination that the programs provide reasonable assurance that FTC information assets are adequately protected, but there are opportunities for improvement. The FTC information assurance and privacy programs continue to evolve: Controls are being added and enhanced to address threat, vulnerability, and requirements changes; Planning practices are being enhanced to incorporate security and privacy requirements at all levels of information system planning, from enterprise to individual system; and Continuous monitoring practices are being instituted to provide FTC management with the current status and "health" of the FTC information assurance and privacy programs.