April 2013

INFORMATION SECURITY

Evaluation of FTC's Information Security Program and Practices for Fiscal Year 2012

Why We Did This Study

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies 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 FTC Office of Inspector General contracted with Allied Technology Group, Inc. to conduct an evaluation to assess (1) the effectiveness of the FTC's information assurance and privacy programs and (2) agency compliance with OMB and National Institute of Standards and Technology (NIST) guidance. (A full report on our evaluation was prepared for FTC internal use only).

What We Found

The IG FISMA evaluation showed that the FTC is in substantial compliance with applicable security and privacy requirements.

FTC programs do, however, require improvement and must evolve as threats and system use changes. The IG recommendations for improvement of FTC security and privacy programs are focused in security planning (e.g., capital planning, enterprise analysis of security needs, and communicating security and privacy performance). FTC reactive security measures are strong, but they need to be augmented with planning and risk-based decision procedures that minimize use of limited resources to protect its information resources (hardware, software, and data).

FTC has been evolving its information security program toward the NIST risk-based model. The changes made in FY 2012 have resulted in a stronger program. They also laid the foundation to resolve the planning deficiencies and contractor management weaknesses previously identified. FTC will need to build on the governance procedures that are now in place to establish the efficient, risk-based information security program that it will need to expand its use of IT to support its missions while continuing to reduce the potential that its systems or associated data can be compromised.

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 the information security continuous monitoring program.