INFORMATION SECURITY


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.