Office of Inspector General

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

August 2016

In accordance with Section 406 (b) of the Cybersecurity Act of 2015, the Federal Trade Commission (FTC) Office of Inspector General (OIG) has completed and submitted the required report on the Federal Trade Commission's (FTC) Covered Systems. This redacted version of the report has been prepared for public release.

The OIG contracted with TACG, LLC to collect and assess the information addressed in the Cybersecurity Act and prepare this report. The contractor's approach was to submit the questions contained in the Cybersecurity Act to the system owners for FTC Covered Systems. The information received was reviewed for accuracy and consistency by comparing responses against information obtained through OIG Federal Information Security Modernization Act (FISMA) assessments. The results of TACG's analysis are provided as responses to the specific questions posed in the Act. However, neither TACG nor the OIG independently verified through testing or performance audit that Covered Systems are operating as intended under the referenced policies.

The results of the review were presented to FTC management prior to issuance of this report. Management concurred with the contents of the report.

OIG Report on the FTC's Covered Systems under the Cybersecurity Act of 2015

Federal Trade Commission

Office of Inspector General

August 12, 2016

In accordance with Section 406 (b) of the Cybersecurity Act of 2015, the Federal Trade Commission (FTC), Office of Inspector General (OIG) hereby provides the required Report on Covered Systems.

The OIG submitted the questions contained in the Cybersecurity Act to the System Owners for FTC Covered Systems. The information received was reviewed for accuracy and consistency by comparing responses against information obtained through OIG Federal Information Security Modernization Act (FISMA) assessments (e.g., System Security Plans, security and performance monitoring reports, and contracts for Covered System support). The results of the OIG analysis are provided as responses to the specific questions posed in the Act. However, the OIG did not independently verify through testing or performance audit that Covered Systems are operating as intended under the referenced policies.

The Cybersecurity Act requires that the OIG provide information about selected security controls applied to Federal computer systems that allow access to Personally Identifiable Information (PII), a "Covered System." The FTC maintains a system inventory that identifies systems that contain PII. The FTC uses a conservative approach in deciding whether a system should be defined as having PII. Specifically, under FTC policy, a system is treated as if it contains PII if there is a potential that it might contain PII. For example, an individual might include PII in a free-form information submission to the FTC, even though PII was not requested. As of June 30, 2016, the FTC had 60 computer systems that in its view meet the definition of a Covered System.

FTC Covered Systems include systems that are owned and operated by the FTC (39 systems), systems that are contractor owned and operated but are dedicated for FTC use (6 systems), systems operated as shared services by other Federal agencies (6 systems), and commercial shared systems (9 systems). The responses provided in this report encompass all 60 systems.

(A) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed

The FTC has a single access control policy that governs the establishment and maintenance of logical access control to all systems -- Covered Systems and non-Covered Systems -- that are operated or used by the FTC.[1] The FTC policy is derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. The policy is reviewed and updated on an annual basis and is current with SP 800-53 Revision 4.

The FTC logical access policies require that systems owners manage information system accounts to include:

- Hardening systems using approved Security Technical Implementation Guides (STIGs)
- Identifying account types within the access control directory structure (i.e., individual, group, system, application)

[1] OCIO 12-AC-100, *Access Control Policy*; OCIO 12-IA-100, *Identification and Authentication Policy.*

- Establishing conditions for group membership
- Identifying authorized users of the information system and specifying access privileges
- Requiring appropriate approvals for requests to establish accounts
- Review, in conjunction with administrators and developers, information system accounts monthly to disable or remove accounts no longer required and to modify access control properties as necessary to align with the job functions of account holders
- Granting access to the system based on: (1) a valid access authorization; (2) intended system usage; and (3) other attributes as required by the organization or associated missions or business function
- Assigning minimum access privileges based on role
- Requiring two-factor access for remote access
- Requiring two-factor authentication for privileged access

The FTC reviews the logical access arrangements at least annually for all supporting computer systems as part of its Assessment and Authorization process. Control measures are revised as necessary to accommodate business needs and to ensure an appropriate security environment. For example, the FTC infrastructure currently uses single-factor access for non-privileged users. The FTC also operates a Secure Investigations Lab (SIL) that, although supported by the FTC Data Center, requires two-factor authentication for all access; and commercial services have adopted cloud-based two-factor authentication approaches that allow identification of multiple mobile devices (e.g., cell phone or tablet) as tokens for a single user.

Based on the results of its controls review as part of its Assessment and Authorization process, FTC issues an Approval To Operate (ATO) for systems that comply with appropriate FTC security and privacy policies and NIST guidance and provide appropriate levels of security and privacy for FTC information assets (hardware, software, and data). The ATO review ensures that FTC systems controls comply with appropriate standards and guidelines.[2]

(B) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users

The FTC requires enhanced access controls for privileged users. Controls listed are in addition to the controls applied to normal system users. The controls are designed to limit access to system functionality and data through administrative procedures and technical controls to specific individuals or computer processes performing administrative functions. Privileged user access controls are evaluated as part of the FTC ATO process and are incorporated into FTC continuous monitoring practices. This ensures that controls tailored for different technologies and business needs provide equivalent, appropriate levels of control.

Among the controls applied to privileged users are:

- Limitation on the number of individuals assigned privileged access

[2] OCIO 14-CA-100P, *Assessment and Authorization Procedures*; OCIO 11-310-01, *Development and Maintenance of Inventory of Major Information Systems.*

- Assigning individuals with privileged access to special directory access groups
- Regular review of privileged accounts and disabling accounts that are no longer in use or needed
- Ensure that privileged user activities are logged and that such logs are reviewed as an on-going Continuous Monitoring practice
- Restricting privileged users to specific devices (e.g., servers) and files (access control lists, access control matrices)
- Firewall and Intrusion Protection System (IPS) restrictions
- Multi-factor authentication that is SP 800-63-2, *Electronic Authentication Guideline*, level 3, using a hardware authentication device or level 4 compliance methodologies including:

    - Personal Identity Verification (PIV) card
    - UserId/password plus physical token/access code
    - UserId/password plus cloud-based token/access code

(C) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication

FTC policy requires that all systems use logical access control to restrict access to system functionality and sensitive data, including PII. Multi-factor authentication is required for privileged users.

(D) A description of the following information security management practices used by the covered agency regarding covered systems:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software

The FTC inventories and monitors software and software licenses for the 39 systems it owns and operates. Responsibility for maintaining appropriate software licensing for the remaining 21 systems is retained by the system owners for those systems. The FTC includes clauses in contracts for the 15 commercial suppliers supporting Covered Systems that they are expected to maintain effective configuration control and management of software used to support FTC operations (e.g., NIST SP 800-53 R4, *Information System Component Inventory*).

The 39 systems owned and operated by the FTC adhere to OCIO-12-CM-100, *Configuration Management Policy*. This policy requires that System Owners maintain a list of software programs authorized to execute on the information system. Users of FTC information systems are prohibited from installing software on any FTC information system unless explicitly permitted.

Information included in the system component inventory includes documentation that:

- Accurately reflects the current information system;
- Is consistent with the authorization boundary for the information system;
- Is at the granularity necessary for tracking and reporting;
- Includes information such as original purchase date, product name, version, licensing information, owner, keys, maintenance requirements, etc.; and
- Is available for review and audit by System Owners and Office of the Chief Information Officer (OCIO) personnel.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) data loss prevention capabilities;

The FTC employs a Web filter to monitor information transiting to the Internet and alerts when or if unusual volumes of data leave the Data Center.

The SIL has information with higher sensitivity than other FTC data. The SIL is isolated from the FTC's production, development, and test lab networks and can only be accessed via VPN [redacted]. Data moving in or out of the SIL must be authorized, the authorization documented, and only SIL administrators may move data in or out of the SIL. SIL data movement is logged.

Other techniques used within Covered Systems include:

- Intrusion Detection Systems (IDS), with [redacted] and User session rate limiting using [redacted];
- Ports and protocol restrictions;
- Log monitoring with forensic review of system activity;
- [redacted] and [redacted] for monitoring both internal and external traffic;
- User and data access pattern monitoring; and
- Application audit logging and monitoring.

(II) forensics and visibility capabilities; or

The FTC uses [redacted] / [redacted] product to collect information about security and performance of its infrastructure systems. The product is used to support cross-domain analysis.

The FTC uses Department of Homeland Security (DHS) services to scan its infrastructure network for vulnerabilities. The Cyber Hygiene Assessment that DHS provides is used to identify areas requiring remediation.

(III) digital rights management capabilities.

A commercial service provider acquired, but has not yet installed [redacted]'s Digital Rights Management suite.

An FTC technical lab is scheduled to implement Digital Rights Management capabilities in September 2016. This capability uses [redacted].

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

For its infrastructure systems,

- The FTC collects information and provides various displays to support identification of performance problems and potential security issues. These metrics are analyzed and displayed using a dashboard approach that facilitates identification and communication of potential anomalies and potential security issues.

- The FTC is using cross domain analysis to analyze infrastructure performance and identify potential security vulnerabilities.

- The FTC monitors information transiting to the Internet via the Web filter. The Web filter blocks known malicious websites and websites that are not allowed by policy, e.g., cloud storage or mobile file access websites. The Web filter retains log information for a period of one year. This log data can be used for forensic analysis.

(iv) If the covered agency is not utilizing capabilities described in clause D(ii), a description of the reasons for not utilizing such capabilities

The only capability described in the response to clause D(ii) that FTC is not using is Digital Rights Management (DRM). DRM is a systematic approach to copyright protection for digital media. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy purchased content. DRM is a mechanism that may be used to protect digital copyrights under the Digital Millennium Copyright Act (DMCA) of 1998.

The FTC has little utility for DRM in its normal operations. The FTC does not issue products where it would be a copyright owner and require DRM protection, and publicly available reports do not warrant DRM overhead. DRM would have limited utility as a potential protective control for information FTC shares with its business partners. In those instance where FTC shares information, it is typically in a mode where the shared data is to be manipulated and analyzed as part of ongoing litigation or other analysis. Typical DRM implementations are intended to restrict such use.

The FTC has strict policies and procedures that govern and restrict the installation of software products that would be subject to the DCMA and would thus not be a viable consumer of such products.

(E) **A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D)**

The FTC Office of the Chief Information Officer issued an *Acquisition Strategy for Information Technology* in 2011. The Acquisition Strategy identifies the policies and procedures to follow in planning for and acquiring IT goods and services. The strategy has a security/privacy focus designed to ensure that contractors are adequately informed as to their responsibilities to protect FTC IT assets (hardware, software, data). As part of the acquisition planning process, security requirements are documented and a determination made as to whether the contractor is to implement an FTC solution or develop a solution. Security and privacy requirements are extracted from planning documents to solicitation documents and, ultimately, to the executed contract.