District of Columbia Paperwork Reduction and Data Collection Act of 2017, Bill 22-574

Before the Committee on Government Operations

The Honorable Brandon T. Todd, Chairperson

June 6, 2018, 10:00 a.m.
Room 412, John A. Wilson Building

Comments by
Keith J. Richardson
Deputy Chief Financial Officer
Office of Tax and Revenue

Jeffrey S. DeWitt
Chief Financial Officer

Thank you for the opportunity to comment on Bill 22-574, the District of Columbia Paperwork Reduction and Data Collection Act of 2017 (“the Bill”).

The Bill was introduced on November 7, 2017 and proposes to create the Data Sharing and Paperwork Reduction Advisory Council (“Advisory Council”). The Advisory Council would advise the Mayor, the District of Columbia Council, and District agencies in developing and implementing process to store and access records electronically, rather than storing physical copies of these records. Prior to implementing any new process, it must be noted that due to agreements with the Internal Revenue Service (“IRS”) only the Office of the Chief Financial Officer (“OCFO”) is authorized to access and obtain Federal Tax Information (“FTI”) data.

The records of the Office of Tax and Revenue (“OTR”) contain FTI. Accordingly, OTR must comply with the security standards set forth in IRS Publication 1075 (“Publication 1075”), as published by the IRS Office of Safeguards. IRS Office of Safeguards security standards require that FTI data not be shared with any office outside of those OCFO offices that have been specifically designated to receive FTI data. Those offices, in turn, are subject to regular IRS Office of Safeguards review. Contractors and subcontractors of the OCFO are subject to these stringent safeguards as well.

Policy and Procedures

OTR has security policies and procedures that cover IRS Publication 1075 requirements for handling case records. OTR has training around these policies and procedures to ensure that everyone adheres to the policy and that they are held accountable for their actions if they do not follow the policy.

Labeling FTI

The outside of the case file that contains FTI is clearly labeled “FTI” so that an individual knows they are accessing FTI before they open the file or record. This means that the outside of the case record is labeled to identify FTI contained within, and every document within the case file that has FTI is clearly labeled.

Implementing this requirement to label an electronic case file as containing FTI from the outside of the file in an electronic environment is currently the biggest challenge to complying with IRS Publication 1075 requirements for electronic case records.

Logging

FTI contained in electronic case records is considered converted media as defined in IRS Publication 1075, Section 3.4, and requires tracking from creation to destruction of the case record. All converted FTI is tracked on logs containing the data elements detailed in Section 3.3. This requires that all documents received from the IRS are identified by:

- Taxpayer name;
- Tax year(s);
- Type of information (e.g., revenue agent reports, Form 1040, work papers);
- The reason for the request;
- Date requested;
- Date received;
- Exact location of the FTI;
- Who has had access to the data; and
- If disposed of, the date and method of disposition.

Auditing

Within the case management application, auditing is enabled to capture access, modification, deletion, and movement of FTI by each unique user. Audit records identify each and every interaction with FTI for the entire period it is in the system. For example, if an Excel spreadsheet containing FTI is loaded into the electronic case record, and it is accessed or downloaded by an employee to take action, the event of accessing or downloading that FTI file is recorded in the audit trail to capture the action taken and the user that took the action.

System Configuration

The backend servers that run the electronic case file system (e.g., application servers and database servers) are secured per IRS Publication 1075 and are accessible to only authorized users. IRS Publication 1075 policy is met by utilizing the Safeguards Computer Security Evaluation Matrix ("Evaluation Matrix") to configure the security settings. These Evaluation Matrices are available for download from the IRS Office of Safeguards web site[1]. Additionally, backup servers, where FTI in electronic case records are backed up for archive, meet IRS Publication 1075 security requirements.

[1] http://www.irs.gov/businesses/small/article/0,,id=177651,00.html

Requirements for FTI in a Web Portal Environment

To utilize a web portal that provides FTI over the Internet to a customer, OTR follows these requirements:

1. Three-Tier Architecture: The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI and access to the database through the application is limited.
2. System Hardening: Each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the web portal is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing.
3. Identity Verification and Authentication: Access to FTI via the web portal requires a strong identity verification process. The authentication uses a minimum of two pieces of information although more than two is recommended to verify the identity. One of the authentication elements is a shared secret only known to the parties involved and issued by OTR directly to the customer. Examples of shared secrets include: a unique username, PIN, password or passphrase issued by OTR to the customer through a secure mechanism. The case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

Three-Tier Architecture for Web Portal Environments

The physical separation of systems into a tiered architecture increases security of the environment because additional layers will be traversed to gain access to FTI. In a situation where the web server, application server and database are located on the same host but logically separated, if that host is compromised, all three tiers are vulnerable.

The first tier (“Web Tier”) consists of the web server that is presenting the web pages to OTR customers and accepts requests. Systems within this tier are the most vulnerable to attack because they are exposed to the Internet. All connections from the web server to the customer over the Internet that contain FTI are encrypted, i.e., HTTPS.

The middle tier (“Application Tier”) is where the business logic resides, and the processing of data and customer requests occurs on an application server. This tier provides a layer of protection between the customers on the Internet and the FTI stored in OTR’s database.

The backend tier (“Database Tier”) is where the database server is contained that stores the FTI. No requests are made from the Internet directly to the backend database with FTI.

A firewall is placed between customer on the Internet and the Web Tier to filter traffic from the Internet to the web server. The second firewall is placed between the Application Tier and the Database Tier to filter requests from the application server to the database.

Access to the database from the application is restricted to specific database tables, rows and columns that contain FTI and that access is read only. There is no ability to overwrite data in the database from the application.

System Hardening

Each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the web portal is hardened in accordance with IRS Publication 1075 policy. This policy can be satisfied by utilizing the Evaluation Matrix to configure the security settings for the applicable operating system of the web server, application server and database server.

Additionally, when FTI is provided to customers through a web portal, the required frequency with which agencies conduct vulnerability scanning of the web portal architecture is increased to monthly to allow for more proactive vulnerability management of systems that provide FTI over the Internet.

In addition, there are other resources available specific to web servers and web sessions that supplement the Evaluation Matrices and ensure the FTI is secured properly in the web portal environment:

National Institute of Standards and Technology Special Publication 800-44, Guidelines on Securing Public Web Servers provides guidance for deploying, configuring, and managing secure web servers. Defense Information Systems Agency publication, Web Server Security Technical Implementation Guide, provides guidance on the technologies used to ensure the appropriate level of protection for web server connections, e.g., Secure Sockets Layer/Transport Layer Security.

Identity Verification and Authentication

Identity Verification and Authentication: Access to FTI via the web portal requires a strong identity verification process. The authentication uses a minimum of two pieces of information although more than two is recommended to verify the identity. One of the authentication elements is a shared secret only known to the parties involved and issued by OTR directly to the customer. Examples of shared secrets include: a unique username, PIN, password, or passphrase issued by OTR to the customer through a secure mechanism. The case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

Two-factor authentication is applicable to employees and contractors, including system and application administrators with access to FTI through a web portal from a network external to OTR's network. This does not apply to the OTR's customers who access FTI through a customer service web portal. All OTR employees and contractors accessing FTI data remotely from an external network through an Internet web portal are required to be authenticated by an application that utilizes a two-factor authentication mechanism. Two-factor authentication (strong authentication) is defined as using at least two out of the three authentication factors: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Using strong authentication provides more protection for FTI than a simple username and password can provide.

Conclusion

The IRS Office of Safeguards reviews the labeling of FTI through the OTR's submission of two reports: the Safeguard Security Report, filed annually, and the Corrective Action Plan, filed twice a year. These reports provide a basis for IRS Office of Safeguards to approve or disapprove the labeling of FTI. Furthermore, under two existing Memoranda of Understanding between the IRS and the OCFO (2007 and, as amended in 2009), only the OCFO is authorized to obtain FTI data. Internal Revenue Code Section 6103(d).