Fairfax County Internal Audit Office

Department of Housing and Community Development
Data Classification Audit
Final Report

November 2019

NOTE: ***Selected sensitive and confidential operational and security information will be omitted from public disclosure, based on the Virginia Freedom of Information Act (FOIA) Va. Code Ann. 2.2-3705.2(14)(b). This information, if disclosed, would subject the County to potential computer data security risks.***

"promoting efficient & effective local government"

Background

Agencies within the Fairfax County Government are responsible for handling sensitive and confidential information during the normal course of operations. County agencies are required to determine data classifications for information processed in County information systems, based on County, legal, and regulatory requirements. Data classifications are used to determine the nature and extent of security and system controls that must be implemented to protect data in information systems. The County Department of Information Technology (DIT) *Information Technology Security Policy 70-05.01* defines four pre-determined classes of data. The four classes are confidential, sensitive, internal use and public use. Confidential or sensitive information stored in County information systems includes data such as client, patient health, Social Security Number (SSN), social services and domestic violence information. Several county agencies are required to comply with *Health Insurance Portability and Accountability Act (HIPAA)* and *Virginia codes* 63.2-104 and 63.2-104.1 for protection and security of social services and domestic violence information. The Internal Audit Office has developed a standardized audit plan to review on a regular basis internal controls over data classification and security of confidential or sensitive information used and stored at individual departments/agencies.

Executive Summary

Our audit focused on determining whether policies and procedures were established for classifying the Department of Housing and Community Development's (DHCD) data based on the level of sensitivity. Additionally, we focused on determining whether DHCD had controls in place to protect confidential records. Finally, we reviewed access to information to ensure it was based on a business need with least privileges access rights. Our audit population included all systems used by DHCD.

DHCD uses multiple application systems to store and manage client information and financial records; however, their main system is Yardi which is a cloud-based management software. It contains confidential/sensitive data such as client information, property information and, waitlist information. Yardi allows for user's access to be restricted not only by security level but also by the user's client properties. We noted that DHCD had access controls in place for the management systems, user access was reviewed annually, and disclosure of data was properly authorized and complied with County policies and external regulations. However, we noted the following exceptions were controls could be strengthened:

- There was no documented process for access requests and approvals for the loan management system, Mitas Group Inc. system (MITAS) and Box.com which is used by the State Rental Assistance Program (SRAP) to transfer data.
- The Data Loss Prevention (DLP) procedures did not require the Agency Information Security Coordinator (AISC) to review the Enforce Console on a regular basis.
- The door to the server room was propped open and the servers were not physically secured.

- Four temporary employees' Yardi access was not deactivated in a timely manner.

Scope and Objectives

This audit was performed as part of our fiscal year 2019 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The objectives of the audit were to determine that:

- Data classification and evaluation was performed in compliance with County Information Security Policy and external regulations.
- Proper controls existed over access and changes to confidential and sensitive data.
- Controls were in place to prevent unauthorized disclosure of confidential information.
- Information was maintained in compliance with county regulations or policies.

Methodology

Our audit approach included the review of *Information Technology Security Policy 70-05.01*; *Best Practice for Records Management – Principles for the Collection, Use and Care of Personally Identifying Information*; the *U.S. Department of Commerce - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII); NIST SP 800-123 Guide to General Server Security; and NIST SP 800-146 Cloud Computing Synopsis and Recommendations* to gain an understanding of data classification determination methodology and best practices for protecting confidential data. We interviewed department management and staff responsible for data classification policies and procedures, system user access, and protection of sensitive or confidential data.

In addition to reviewing the Yardi system's internal controls, we reviewed procedures surrounding the other systems which contained confidential/sensitive information utilized by DHCD. We conducted system walk-throughs, reviewed user requests for access, the removal of access for terminated/transferred employees, and determined if access was appropriate for users. For data hosted by third party vendors, we reviewed the contracts to determine if there was language which described the methodology for the return or destruction of sensitive data once the contract was terminated.

The Fairfax County Internal Audit Office (IAO) is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the County Executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and IAO reports are available to the public.

Findings, Recommendations, and Management Response

1. Access Request Form

DHCD IT Systems Access Form did not include granting access to MITAS or SRAP. MITAS is a loan management program with four users. While the access to the system was assigned based on job responsibility, there was no documented approval of the current users' access. The SRAP program uses Box.com to transfer data between DHCD and the Virginia Housing Development Authority. A ticket was submitted to DIT to allow the users to access Box.com within the County network; however, there was no formal access request form to document the approval of access.

Information Technology Security Policy 70-05 01, Section 3.5.1 Access Control states: "Authorization to create a user ID and password must be received from a designated approval authority. Requests for user, administrative, and system access must be approved according to formal access request procedures." In addition, "Authorization to create a user ID and password must be received from a designated approval authority. Requests for user, administrative, and system access must be approved according to formal access request procedures."

Additionally, *NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, Section 4.3 Security Controls* states: "Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists)." A form of access control is to document the appropriateness of the access granted to individuals, this is best done through the completion and approval of an access request form. This will evidence the need for access and the approval of the access.

Recommendation: We recommend DHCD revise their existing IT Systems Access Form to include granting access to MITAS and SRAP (box.com). This should require the employee's supervisor and the Security Access Administrator's approvals prior to Information Systems & Services (ISS) granting access to the system. This would ensure that access to these systems is limited to only individuals who require access to the confidential information and document the reason for the granted access.

Note: During the audit, IAO verified that DHCD updated the IT Systems Access Form to include granting access to MITAS system and SRAP program. Moving forward all requests to access for MITAS and SRAP will be documented and retained for future review. No follow-up is needed for this item.

2. Data Loss Prevention (DLP) Procedures

DHCD's DLP Policy did not require the AISC to review the DLP dashboard on a regular basis. Per DIT policy, *Incident Remediation Procedures for AISCs – Data Loss Prevention*, "The Agency Information Security Coordinator (AISC) is responsible for reviewing and remediating their department's DLP incidents. This includes, but (is) not limited to…review(ing) and remediat(ing) DLP incidents in the Enforce Console."

NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information, Section 4.1 Operational Safeguards states "As agencies work to establish a variety of safeguards to protect the confidentiality of PII, they must also ensure that mechanisms are in place to make certain that individuals are held accountable for implementing these controls adequately and that the controls are functioning as intended. Additionally, *section 4.3 Security Controls* states: "Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. An example is the use of data loss prevention technologies."

If the DLP Enforce Console is not reviewed on a regular basis, incidents not detected by DIT ISO could go uninvestigated for an extended period. These incidents could contain up to 50 social security numbers or 10 full credit card numbers. DIT only has the resource capacity to notify departments when an incident reaches certain medium/high risk criteria thresholds.

Recommendation: We recommend DHCD update their DLP Procedures to require the AISC to review all incidents in the Enforce Console on a regular basis to ensure that possible data breaches do not go undetected for a significant period.

Note: During the audit, IAO verified that DHCD set up a report in the DLP console that shows all new incidents. This report is emailed to the IT Manager and auto forwarded to the AISC twice a week, Wednesday and Friday. The AISC reviews and clears all instances of personal use/false positives on a weekly basis. If it appears that a breach occurred, the AISC will review the incident in the consul and take immediate action. DHCD has updated their DLP procedures to include the stated process. No follow-up is needed for this item.

4. Server Room Security

The room where servers were stored was not secure. The temperature control system was not functioning and to keep the room at a temperature which allowed the servers to operate, the door to the room was propped open. The door to the server room was equipped with a cypher lock, but since the door remained open anyone who had access to the floor could also have direct physical access to the servers. One of the purposes of the servers, stored in this room, is to secure Yardi reports prior to uploading them to HUD.

Per *Information Technology Security Policy* 70-05.01, *Section 2.10 Physical and Environmental Protection* states: Facilities that host critical information system should be a secure environment with access restricted to authorized personnel." Additionally, *DIT INFOSEC Standard Operating Procedures (SOP)-100-02 – System Harding Standards* states: "Information Technology systems are used by county to supply critical functions to both county and constituents and employees. These systems must be protected from both internal/external security and performance associated risks."

Additionally, *NIST SP 800-123 Guide to General Server Security, Section 3.1*

Installation and Deployment Planning states: "Many servers host sensitive information…In such cases, it is critical that the servers are located in secure physical environments.

Ineffective access control procedures increase the risk that confidential data could be improperly accessed, modified, or copied. By allowing unauthorized individuals direct access to servers, there is an increased risk that the hardware could be damaged, intentionally or accidentally.

Recommendation: We recommend the servers be secured behind a locked door at all times with access minimized. The temperature control unit which services the server room should be either repaired or replaced so the room temperature can be properly maintained to allow the servers to operate normally.

Note: IAO verified that the servers have since been moved to the secured DIT server room and are no longer stored on site at DHCD's offices. No follow-up is needed for this item.

5. Yardi Access Termination

Four temporary employees' access to Yardi was not removed in a timely manner after their contracts expired. Three of the employees' contracts ended on June 30, 2019, and one ended on May 21, 2019; however, they continued to have access through July 23, 2019.

Information Technology Security Policy 70-05 01, County Agencies' & Other User Entities Involvement and Responsibilities states: "The administrator is responsible for validating immediate termination of user privileges when workers change jobs or leave the County."

Additionally, *NIST SP 800-123 Guide to General Server Security, Appendix D – Fair Information Practices* states: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."

If a user's credentials are still active after they leave the county/department there is a risk they could access, tamper with, and steal sensitive and confidential client information.

Recommendation: We recommend DHCD implement procedures for the deactivation of temporary employee accounts in YARDI immediately after their contract expires, or they are terminated or transferred.

Management Response: DHCD is working on a SharePoint onboarding form/offboarding form that must be completed upon departure. This form will be required for all temporary staff which will require deactivation of credentials upon departure from the agency. The anticipated completion date for this is February 2020.