Fairfax County Internal Audit Office

Office of Human Rights and Equity Program (OHREP)
Data Protection Audit
Final Report
March 2022

"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. Departments and agencies are required to determine data classifications for information processed in County information systems, based on County policies and state and federal legal/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 (IT) Security Policy 70-05.01v8* 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 personally identifiable information that are associated with allegations of discrimination, patient health, Social Security Number (SSN), social services and domestic violence information. Multiple 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 (IAO) has developed a standardized audit plan to review on a regular basis internal control over data classification and security of confidential or sensitive information used and stored at individual departments/agencies.

Executive Summary

Our audit focused on controls over classifying department's data based on the level of sensitivity and their controls to protect confidential records. Additionally, we reviewed access to information to ensure it was based on a business need with least privileges access rights. Our audit population included the four systems Office of Human Rights and Equity Program (OHREP) operates, three of which are third party systems.

OHREP uses the County owned Intranet Quorum System (IQ) to document investigations of discrimination cases for employment, housing, and public accommodation. OHREP also uses two third party systems that are federal owned case management systems (Integrated Mission System (IMS) and HUD Enforcement Management System (HEMS)) to track employment, housing, public accommodation discrimination cases investigated by the OHREP staff on behalf of the Equal Employment Opportunity Commission (EEOC) and Housing Urban Development (HUD) respectively. Lastly, OHREP uses the federal owned Line of Credit Control System (eLOCCS) for HUD programs grant reimbursement.

OHREP staff was knowledgeable of *IT Security Policy 70-05.01v8* to protect data processed on the County owned systems. Users access rights to systems were granted based on their job responsibilities. Physical case files were secured in locked cabinets. And, OHREP implemented proper informal controls over access and changes to confidential and sensitive data. Disclosure of data to external entities was properly authorized and complied with County policy and external regulations. OHREP will strengthen their internal control effectiveness in the following ways:

- Remove from IQ, IMS, HEMS and Zoom seven account users that are no longer department employees by working with Department of Information Technology and 3rd party system owners.
- Develop and implement formal written procedures for requesting staff access or removal from systems including identifying which staff can initiate and approve requests; properly removing terminated staff; and retaining records of access requests/changes for IQ, IMS and HEMS systems. OHREP has initiated and implemented a systems security roles and access policy. After the completion of the audit EEOC replaced the IMS system with Agency Records Center therefore policies and procedures were developed for the new system instead.
- Perform periodic review of the user lists for the IQ, IMS, HEM systems and the department Zoom account to ensure user access is aligned with employees' job responsibilities. Documentation of OHEP's performance of this review will be maintained in their system access management files.
- Develop formal policies and procedures that require the use of appropriate Microsoft Outlook encryption measures to minimize the risk of the unauthorized disclosure when emailing confidential information to federal partners. OHREP has trained staff on the required encryption settings and is working on formalizing their guidance in writing.
- Ensure OHREP's Zoom meeting security settings comply with DIT guidance while the application is still in use. Additionally, OHREP will be transitioning to solely using to MS Teams before the end May.
- Conduct an inventory of the USBs purchased and ensure those not in use are properly sanitized. OHREP inventoried and sanitized/reformatted six (6) Kingstone Flash Drives in current inventory. OHREP management reinforced with the AISC his/her responsibilities, per their policy, the requirement to use of the "Kingstone Flash Drive Sign-out Sheet" when issuing USB drives.

Scope and Objectives

This audit was performed as part of our fiscal year 2021 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 the adequacy of controls over:

- Development of Office of Human Rights and Equity Program data protection processes for the period March 1, 2020, through March 31, 2021;
- Compliance to County Information Security policy and external regulations for data identification, classification, and protection for all systems;
- Access and changes to confidential and sensitive data;
- Disclosure of data.

Methodology

Our audit approach included review of *Information Technology Security Policy 70-05.01 v8*, 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, Policy and Procedures for Portable Storage Devices (USB Flash Drives)* and other online meeting tool policy and procedures 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, practices for the disclosure, and protection of sensitive or confidential data. We obtained a list of the systems the OHREP operates and determined the reasonableness of data classification. In addition, we conducted system walk-throughs, reviewed user requests for access and removal of access for terminated/transferred employees, determined if access was appropriate for users, and reviewed system audit trail logs.

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 audit reports are available to the public.

Findings, Recommendations, and Management Response

1. IQ System User Access

OHREP uses the Intranet Quorum System (IQ) to document the investigation of discrimination cases for employment, housing, and public accommodation. There were no formal, written processes for granting OHREP staff access to IQ. Informally, OHREP Supervisors sent IQ user access requests (add, change, or delete user) to a dedicated DIT help desk email address. We found OHREP did not retain all the access request email communications sent to IT help desk. OHREP provided copies of 3 new users' access requests that were process in May 2019 (1) and July 2021(2). The system currently has 18 active users.

Additionally, OHREP reviews the IQ system user list on a semi-annual basis to ensure users' access is proper. We noted that 3 out of 18 users should be removed from IQ, the departure of these 3 users occurred in between the review period.

User	Role	Reason for Removal
User 1	Investigator	Transferred from OHREP July 2021 (*same user in IMS*)
User 2	Investigator	Left County Employment August 2021 (*same user in HEMS*)
User 3	Investigator	Left County Employment September 2021 (*same user in IMS*)

Access to IQ is via a single sign-on process that only permits the user to access the application if they have a valid county logon ID. The two employees that left County employment no longer had access to IQ because their county logon IDs were suspended. However, their active accounts would be considered a security vulnerability for an insider threat or if a hacker were to breach the County's network security. The employee who transferred to another department still had access to IQ by maintaining a county logon.

Per *IT Security Policy 70-05.01v8* - "*3.5.2 Account Administration Requests for County information system accounts shall maintain a formal and valid access authorization based on approved intended system usage within personnel mission and business functions… User access to Fairfax County systems shall be periodically reviewed and adjusted as necessary by the system owners to ensure that access is in accordance with the concept of least privilege. Agency Information Security Coordinators, Agency Access Control Administrators, or other designated personnel shall review and adjust access privileges when the role or responsibilities of a user changes or the user no longer needs access to County information systems or applications*."

Not having a formal process for ensuring compliance with the information technology governance documents increases the likelihood of inappropriate access and changes in data in IQ, and the risk of data breaches and misuse of confidential/sensitive information.

Recommendation: We recommend OHREP work with the DIT IQ system support to resolve the improper user access noted from the audit. OHREP's authorization to DIT for removing the three users' access rights should be formally documented. Additionally, OHREP should develop a written, formal procedure for staff requesting access to IQ including approval requirements and maintaining all the user access requests email communications or Service Now IT ticket details. OHREP should train/debrief the applicable supervisors and the department Agency Information Security Coordinator (AISC) on the procedures and communicate the formal procedures to DIT IQ system support., OHREP should work with the IQ system support to periodically perform a documented review of the IQ user list to ensure user access to IQ data is aligned with employees' job responsibilities. Lastly, the role of the AISC is to lead the compliance, and implementation of the *IT Security Policy 70-05 01v8.* OHREP's AISC should be notified of changes to staff's access to these systems to be able to confirm proper removal of access rights during employee termination/transfer.

<u>Note:</u> OHREP stated that the recommendations were completed on March 15, 2022. IAO will test the compliance in the future follow up.

Management Response: With the assistance of DIT, OHREP resolved the improper user access noted from the audit. OHREP has trained/debriefed the Unit Supervisors and the department Agency Information Security Coordinator (AISC) on the agency's procedures for requesting access to IQ including approval requirements and formally maintaining all user access requests and modifications. The process has been communicated to DIT IQ system support. OHREP developed and implemented a written, formal policy which details the procedure for staff requesting access to IQ, to include approval requirements and requires maintaining all the user access requests email communications and/or Service Now IT ticket details. The recommendations were completed on March 15, 2022.

2. 3rd Party Systems' User Access

HUD Enforcement Management System (HEMS)

OHREP uses HUD Enforcement Management System (HEMS), a Federal Government /HUD owned case management system, to document housing and public accommodation discrimination complains investigated by OHREP on behalf of HUD. OHREP does not have formal procedures requiring the retention of user access request email communications and performing periodically user list review. We found OHREP did not retain all the access request email communications sent to HUD. For the 11 active users, OHREP provided a copy of 1 new user request that was processed in April 2020.

Additionally, the user list was not being reviewed periodically to ensure users' access are proper. We noted that 2 out of 11 users should be removed from HEMS.

User	Role	Reason for Removal
User 1	User	Left County Employment August 2021*(same user in IQ)*
User 2	Coordinator	Left County Employment July 2021 (*same user in IMS*)

HEMS is a web-based system, therefore, former OHREP employees can still access HEMS if their user access rights have not been terminated.

Note: During the audit, we confirmed that OHREP terminated the user in the HEMS and submitted a request to the HUD helpdesk to terminate the user with the "Coordinator" role.

Integrated Mission System (IMS)

OHREP uses Integrated Mission System (IMS), a Federal Government/US equal Employment Opportunity Commission (EEOC) owned case management system, to document employment discrimination complaints investigated by OHREP. OHREP does not have formal procedures requiring the retention of user access request email communications and performing periodically user list review. We found OHREP did not retain all the access request email communications sent to EEOC. For the 19 active users, OHREP provided 1 new user request that was processed in November 2019, 2 new users' requests that were processed in February 2021, 1 new user request was processed in June 2021, and 1 new user request that was processed in July 2021.

Additionally, user list is not being reviewed periodically to ensure users' access are proper. We noted that 6 out of 19 users should be removed from IMS.

User	Role	Reason for Removal
User 1	Investigator	Transferred from OHREP July 2021 (*same user in HEMS*)
User 2	Investigator	Left County Employment Feb. 2020
User 3	Investigator	Left County Employment Jan. 2020
User 4	Investigator	Left County Employment June 2019
User 5	User	Left County Employment July 2021 (*same user in HEMS*)
User 6	Investigator	Left County Employment Sept. 2021(*same user in IQ*)

Investigator users are added to IMS to allow cases to be assigned to the OHREP staff for EEOC communication purposes, therefore, users with the Investigator role don't have read/write access to IMS. IMS is a web-based system, therefore former OHREP employees with User role, which does allow write access, can still access IMS if their user access rights have not been terminated.

Per *IT Security Policy 70-05 01v8, 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*."

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)*."

Not having a formal process for ensuring compliance with the information technology governance documents increases the likelihood of inappropriate access in the 3rd Party owned systems. If a user's credentials are still active after they leave the county or transfer to another county department, there is risk of data breaches and misuse of confidential/sensitive information. HEMS and IMS are Federal owned systems; reputation impairment may occur if a data breach is cause by the County.

Recommendation: OHREP should work with the HUD and EEOC helpdesk to resolve the improper user access noted from the audit. OHREP authorization for granting and removing the user's access rights should be formally documented. The role of the Agency Information Security Coordinator (AISC) is to lead the compliance, and implementation of the *IT Security Policy 70-05 01v8.* OHREP's AISC should be notified of changes to staff's access to these systems to be able to confirm proper removal of access rights during employee termination/transfer. Additionally, OHREP should develop a formal procedure to retain all the user access requests email communications. OHREP should train/debrief supervisors and AISC on the procedures. Lastly, OHREP should periodically perform a documented review of the HEMS and IMS user lists to ensure user access to HEMS and IMS data is aligned with employees' job responsibilities.

Note: OHREP stated that the recommendations were completed on March 15, 2022. IAO will test the compliance in the future follow up.

Management Response: OHREP, with the assistance of HUD helpdesk, resolved the improper user access noted from the audit. Authorization for granting and removing the user's access rights is formally documented in HEMS and is accessible to all OHREP staff granted Coordinator status. Currently, OHREP has three (3) mangers granted this status. On February 7, 2022, the EEOC terminated the use of IMS to all users and implemented Agency Records Center (ARC). ARC allows OHREP Registration Managers and Approvers (RM/A) to have access to the production environment of ARC and to assign roles to our organization's users. This allows OHREP to maintain user's access without the need to contact EEOC helpdesk. OHREP developed and implemented a written, formal policy which details the procedure for staff requesting access to HEMS and ARC, to include approval requirements and requires maintaining all the user access requests email communications and/or Service Now IT ticket details. The policies and procedures were completed on March 15, 2022.

3. Email Encryption

OHREP sent the Case Payment Package PDF file to HUD via non encrypted email. Personally identifiable information such as the complainant and respondents' name and address that are associated with a discrimination allegation are considered confidential information. This information is in the closure letters, certified mail receipt, and signed determinations that are email attachments. The packages do not include related health information therefore there is a low risk of disclosures that violate HIPPA. Additionally, witness' information and detailed complaint information were documented in the determination letters.

IT Security Policy 70-05.01v8, 3.3 Encryption states "*Encryption mechanisms shall be applied to information in transit across information systems, network infrastructure, and other communications architecture and data at rest on computer readable media when technically feasible to protect the confidentiality and integrity of County information…. Confidential or Sensitive data shall be encrypted during transmission using encryption measures strong enough to minimize the risk of the unauthorized disclosure if intercepted or misrouted".* 4.4 Confidential Information states" *Information classified as Confidential or Sensitive transmitted to external networks shall be encrypted in accordance with DIT encryption standards*."

The Case Payment Package, an email attachment that contains personally identifying information, can be intercepted during transmission, in an unencrypted email. Unencrypted email and any attachments can be read, and potentially copied and forwarded by anyone. Confidential/sensitive information can be exposed.

Recommendation: We recommend OHREP management instruct staff to use the appropriate Microsoft Outlook encryption setting to encrypt message contents and attachments that contain confidential information, such as personally identifying information. OHREP management should develop formal policy and procedures that require the use of encryption measures strong enough to minimize the risk of the unauthorized disclosure. OHREP management should train/brief supervisors, AISC and staff on the requirement for encrypting emails containing confidential data.

Management Response: OHREP management and staff have been trained and instructed on how to use the appropriate Microsoft Outlook encryption setting to encrypt message contents and attachments that contain confidential information, such as personally identifying information. OHREP management will develop a formal policy and procedure that requires the use of encryption measures strong enough to minimize the risk of the unauthorized disclosure when communicating and/or exchanging information or files with Federal agencies. The anticipated completion date is March 25, 2022.

4. Zoom Account Settings

OHREP purchased and set up a Zoom account through DIT in June 2020. OHREP used Zoom for public Human Rights Commissions meetings. We compared Fairfax County Zoom Requirements set forth by DIT in April 2020 to the OHREP Zoom account meeting settings and noted three out of five meeting setting categories do not comply.

Suggested Zoom Meeting Setting	Status	Potential Risk
Disable-Embed password in meeting links	Not disabled	Increased the risk of an uninvited individual joining the meeting by having access to the meeting link, which makes the meeting access insecure.
Disable file sharing options, including the importing of files into the meeting	Not disabled	Increases the risk of malicious content be shared in the meeting. In conjunction with an embed password in the meeting link, can give an uninvited individual the ability to share improper documents.
Disable feedback to Zoom	Not disabled	Increase the risk of disclose participant’s identification information.

The OHREP Zoom account had 3 users, who could schedule zoom meetings. We noted 1 user left County employment in June 2021 and had not been removed from the account.

Note: During the audit, we confirmed that OHREP removed the user.

Fairfax County Zoom Requirements states “*Fairfax County requires the meeting host to follow and implement these settings on each meeting… The host must only share meeting invitations directly to participants via email, SMS, or phone calls. The host must not include any sensitive information in the meeting invitation.”*

Not disabling the 3 identified features increases the risk that uninvited users can access the meeting and files; share unwanted documents during the meeting; and, potentially disclose the participants' private information. If a user's credentials are still active after they leave the county or transfer to another county department, there is risk of unauthorized access to the meetings. OHREP was not aware of the DIT Zoom account settings' requirements.

Recommendation: We recommend OHREP resolve the improper zoom settings noted from the audit or document the reason why the settings cannot be applied. OHREP should compare Zoom meeting settings to DIT guidance periodically to ensure all the settings comply with the DIT guidance. Additionally, OHREP should ensure that staff with Zoom access who leave the department have their county account access terminated immediately and review Zoom user list periodically to ensure only the users who work for the department and have legitimate job responsibility have access to the Zoom account. Lastly, OHREP should periodically review Microsoft Teams functionality to determine if it will meet their operational requirements to replace the use of Zoom as DIT prefers County staff use of MS Teams for video conferencing for better application support and security.

Management Response: OHREP will transition from utilizing ZOOM for Human Rights Commission meetings and utilize the County Recommended Teams. In the interim, OHREP AISC will set all ZOOM settings consistent with Fairfax County IT recommended settings. The anticipated completion date is May 4, 2022.

5. USB Drives

We found that OHREP had a supply of Kingstone flash drives (USB) for which inventory records were not maintained or retained. Per OHREP's USB Flash Drive Policy a "Kingstone Flash Drive Sign-out Sheet" was to be used to log the USB distribution to the staff. Additionally, when staff left the department, they were to be asked to return any USBs held. Per discussion with OHREP, staff have not used flash drives for storing investigation documents for at least 5 years. However, there were no current records detailing how many USBs the department had or who has custody of the USBs. Lastly, per staff there was uncertainty if USBs were retrieved from departing staff or if USBs held were wiped of data.

OHREP uses the DIT suggested "*Policy and Procedures for Portable Storage Devices (USB Flash Drives)"* as its internal policy outlining the acceptable use and handling of the USB thumb drives.

Per *OHREP Policy and Procedures for Portable Storage Devices (USB Flash Drives)* "*The AISC shall be responsible for ordering, issuing and tracking portable storage devices for the agency in accordance with County policies and procedures. Users of portable storage devices shall protect the data against unauthorized access and/or disclosure. Users shall ensure portable storage devices remain free of viruses and malicious code. Loss or theft of portable storage devices must be reported to the AISC* *immediately along with the serial number of the device and a description of the data stored on the device."*

Per *IT Security Policy 70-05.01v8* "*2.7 Media Protection. Agencies shall use an approved media erasing tool to ensure with reasonable expectation that information is overwritten on County information systems, electronic media, and storage devices prior to disposal or reuse. Agencies shall utilize sanitization methods with the strength and integrity commensurate with the classification or sensitivity of the information. Storage media and devices shall be sanitized prior to the release to vendors or maintenance personnel for maintenance to prevent unauthorized disclosure of data."*

OHREP did not follow its internal policy to track and handle the USB flash drives purchased. The department does not know if confidential/sensitive data has been released or exposed on the unaccounted USB flash drives. The flash drives have not been actively used for five years.

Recommendation: We recommend OHREP AISC inventory the USBs the department purchased and make sure those not being used are properly sanitized to wipe out all the data stored on the USBs. OHREP management should reinforce with the AISC his/her responsibilities per the policy especially the use of the "Kingstone Flash Drive Sign-out Sheet" and the need to sanitize/reformat USB after use. The AISC should work with Human Resource (HR) person to ensure USBs are included as one of the County issued devices being sought for return when staff leave the department. Lastly, OHREP should periodically review and update the policy to reflect the current DIT policy.

<u>Note:</u> IAO was able to confirm that five USB Flash Drives that were not in use at time of verification were wiped clean and secured.

Management Response: OHREP management has reinforced with the AISC his/her responsibilities per the policy, to include, if needed, the use of the "Kingstone Flash Drive Sign-out Sheet" and the need to sanitize/reformat USB after use. OHREP has inventoried all six (6) Kingstone Flash Drives in our current inventory. The flash drives have been sanitized and wiped clean. The recommendations were completed on March 15, 2022.