city of
CINCINNATI

Interdepartmental Correspondence Sheet

Date: October 19, 2016

To: Harry Black, City Manager

From: Lauren Sundararajan, CFE, Internal Audit Manager L S

Copies to: Internal Audit Committee
Jayson Dunn, Enterprise Technology Solutions Director

Subject: **Cincinnati Human Resource Information System Security Audit**

Attached is the Cincinnati Human Resource Information System (CHRIS) Security audit report. The primary objective of this audit was to assess internal controls and practices surrounding security of employees' Personally Identifiable Information within CHRIS. This audit was completed in accordance with Internal Audit's current work plan.

We would like to thank management and staff of the Enterprise Technology Solutions Department for their assistance and cooperation during this audit.

If you need any further information please contact me.

Attachment

Cincinnati Human Resource Information System Security Audit

October, 2016

city of CINCINNATI
INTERNAL AUDIT

Lauren Sundararajan, CFE
Internal Audit Manager

Meredith Shores
Internal Auditor

Jennifer Sherman
Internal Auditor

Table of Contents

Executive Summary

Internal Audit (IA) performed an audit of the Cincinnati Human Resource Information System's (CHRIS) security. The audit objective was to assess internal controls and practices surrounding the security of employees' information within CHRIS.

CHRIS contains the personal information of all City employees and, thus, presents a prime target for those seeking to impersonate or exploit others for personal gain. Although CHRIS personnel are not aware of a breach of the system since its inception, maintaining appropriate defenses against unauthorized system access is a constant process due to the continuous advancements in technology. IA compared CHRIS' current practices to the City's Information Security Policy (ISP) and industry best practices to identify areas that provide an opportunity for operational improvements.

IA identified several issues in the documentation and oversight of CHRIS' security policies. The current ISP has not been updated since 2010 and contains practices that are either not applicable or were never integrated into CHRIS' day-to-day operations. The ISP also does not explicitly address CHRIS in any capacity. In addition, there is no Disaster Recovery Plan in place. This severely inhibits the ability of the system to regain functionality following a natural or man-made disaster.

There is also room for improvement in CHRIS' daily functioning. IA determined the procedures for granting access into CHRIS or granting access to City hardware are occasionally documented incorrectly or inconsistently and lack appropriate oversight. Additionally, password policies for approved accounts are excessively lenient and several current practices pertaining to remote access are in direct violation of City policy.

To ensure internal controls over CHRIS security are functioning at an optimal level, IA recommends updating the ISP, creating a Disaster Recovery Plan, amending all applicable access forms, reconfiguring password controls, and verifying the need for remote access. These changes will facilitate verification of active users, provide guidance as to required operations, and reduce the risk generated by unacceptable practices.

I. Introduction

Background

CHRIS is the central access point for all City employees' Human Resource information. Its functions include payroll processing, retention of employee records, health and safety documentation and training records. With over 6,000 City employees, this system presents a prime target for unauthorized individuals seeking to obtain data with malicious intent.

Personally Identifiable Information (PII) is defined as any information that allows one to uniquely identify an individual or identify an individual within a larger context. This could include an individual's social security number, bank account information, date of birth, address or phone number. Once this information is obtained by an unauthorized party, it can be used to the severe detriment of the individual. Consequences of exposed PII range from identity theft to compromises of personal safety. Although it is impossible for any system containing PII to eliminate all threats, it is imperative that a system proactively curtail threats by adhering to recommended industry best practices.

CHRIS is an entity within the City Enterprise (CIT-E) Division of the Enterprise Technology Solutions (ETS) department. There are currently 2.75 employees responsible for the management and upkeep of CHRIS. Although there have been fluctuations in the number of employees over the course of CHRIS' existence, the current staffing level is the lowest since the system's inception.

Users are granted access to CHRIS based on their position's time-keeping process or their assigned duties. Many labor intensive positions require employees enter their hours into CHRIS. These employees do not have access to the personal information of other employees and pose little risk to the integrity of the system. Other user access levels range from allowing an account to view or edit personal information regarding employees within their own department, up through allowing the user to view or edit the personal information of all City employees. Designated privileges range from a read-only access level where the user is able to view, but not edit information, to administrative level capabilities where the user is able to make changes to existing records.

As of July, 2016, there were 1,322 active accounts within the CHRIS system. Of this total, 334 users had the ability to access the personal information of other employees.

Audit Selection

IA conducted this audit as part of the current audit agenda.

Audit Objective

The audit objective was to assess internal controls and practices surrounding security of employees' PII within CHRIS.

Audit Scope and Methodology

In order to achieve the audit objective, internal audit staff compared CHRIS' security practices to relevant City policies and industry standards, sought verification of procedures through documented reports, interviewed staff, calculated statistics of relevant data and reviewed authorization documentation for multiple systems. The time frame corresponding to the authorization documentation ranged from September 2008 through August 2016 and was dependent on the system in question.

Statement of Auditing Standards

As required by the Cincinnati Administrative Code Article II §15, this audit was conducted in accordance with the Generally Accepted Government Auditing Standards (GAGAS), except for standard 3.96 pertaining to external peer review requirements. This exception did not have a material effect on the audit.

IA continues to conduct internal quality reviews to assure the conformance with applicable GAGAS. IA performed the fieldwork between July 2016 and August 2016.

Commendations

Internal Audit commends the staff of the ETS Department for their cooperation throughout the audit.

II. Audit Findings and Recommendations

The City's IT security policies and procedures are outdated, obsolete and not applicable to many functional areas of the system.

Comprehensive IT security policies and procedures assist management with providing direction to staff and are a key component of internal controls. However, Version 3.0 of the ISP was never integrated into daily operations and has not been revised or updated since June of 2010. The current ISP includes procedures and operations that are either not applicable to ETS' current IT assets or are obsolete. Additionally, the policy does not contain practices specific to the CHRIS system as it relates to accessing and maintaining the confidentiality of PII.

The opportunity for unacceptable deviations from standard IT security operating procedures exists when policies and procedures have not been thoroughly updated and communicated to staff. The lack of relevant policies allows supervisors to exercise discretion in determining policies and procedures to follow, increases the likelihood of lapses in security and induces variation in operating procedures across different functional areas.

Recommendation 1: Update the ISP to reflect current operating procedures and industry best practices. This includes creating policies specific to maintaining the integrity and confidentiality of employees' PII within CHRIS. Only practices that the City has intent of enforcing and utilizing and that have been determined to add value to IT operations should be incorporated.

Department Response: Agree. ETS has been unable to permanently fill the Information Security Officer and Security Analyst FTE positions since 2015 due to budget constraints. As a result, the City's Information Security Policy has not been updated since 2005 and is out of date. In the ETS FY17 budget, funding for the ISO and 2 Security Analysts has been restored to the operating budget. The ISO and Security Analyst positions will be filled in Q4 of FY2017. Updating the Security Policy will be an immediate deliverable for the new ISO. The CHRIS technical team and City HR will be consulted to insure that onboarding, off-boarding, and CHRIS information security needs are captured and updated in the refreshed security policy.

Staffing limitations pose risks to the integrity and security of CHRIS.

The number of CHRIS employees has decreased to less than half of the system's original staff level over the system's 17 year existence. These reductions have been the result of the automation of processes, migration to a web-based application and budgetary restrictions. At its initial deployment in 1999, there were approximately 8 employees developing and maintaining the CHRIS system. By 2007, there were 4.75 employees. This number has declined to 2.75 as of August, 2016.

The interviewing of ETS staff suggested the current staffing levels do not allow for adequate resources to be allocated to both maintenance and development of the system. IA found there is one employee responsible for all front-end administration. Additionally, the same personnel who are responsible for development are also responsible for production, a violation of industry best practices. Further, neither the front-end administrative duties nor the production and development activities are able to be verified by other employees due to staffing limitations. The IT Manager overseeing the CHRIS system believes 4-5 employees would allow for improved maintenance and innovation and would enable essential duties to be appropriately segregated amongst employees.

Segregation of duties is a key component of internal controls that reduces the likelihood of error and the risk of fraud and abuse. In order to maintain appropriate segregation of duties, no single employee should have the ability to create, execute and monitor activities within a function. If circumstances do not allow for the proper segregation of duties, mitigating controls may need to be implemented to ensure that a single employee is unable to control an entire process.

Recommendation 2: Consult with HR to determine the appropriate staffing level that will allow for improved system maintenance and ensure the allocation of duties amongst personnel aligns with current IT standard practices.

Department Response: Agree. The CHRIS technical team currently consist of an I.T. Assistant Manager, 2 full-time Computer Systems Analysts, and a part-time Computer Systems Analysts. ETS will evaluate the CHRIS system support requirements and determine if the current CHRIS team roles and responsibilities can be adjusted to allow duties to be segregated, staff to be cross trained, and a succession plan to be implemented to preserve institutional system knowledge due to possible retirements in upcoming years. An additional CSA FTE or professional services resource for the CHRIS team has been budgeted in FY2017.

Recommendation 3: Implement mitigating controls to ensure there is proper segregation of duties for the current staffing level.

Department Response: Agree. See department response to recommendation 2 above.

The Information Security Officer (ISO) position has been vacant for an extended period of time.

An ISO establishes and operationalizes the security policies necessary to protect an entity’s informational assets. Although a strategic position within the organizational framework, the current ISO position has been vacant since November 2015. These duties are currently fulfilled by an IT Manager whose designated position requires overseeing the telecom and fiber network, monitoring ETS’ service desk and providing PC and application support. Requiring one employee to execute the duties inherent to both the ISO position and an IT managerial position increases the likelihood of lapses in the timely execution of duties and shortfalls in maintaining the optimal operation and integrity of the system.

Recommendation 4: Hire an individual who has the ability to fulfill the duties of the ISO position.

Department Response: Agree. See department response to recommendation 1 above.

A Disaster Recovery Plan does not exist and the current physical storage of City hardware could exacerbate the effects of an adverse event.

A Disaster Recovery Plan provides guidance as to the procedures to be followed in the event of a disaster. The ISP requires ETS to create, implement and conduct annual testing of a Disaster Recovery Plan to facilitate business continuity in the case of a natural disaster or intentional system sabotage.[1] However, budgetary limitations and low staffing levels have prohibited the creation and implementation of such a plan, although there is a pending request for funds to address this shortfall.

Industry best practices require physical hardware to be stored in multiple locations to prevent the total loss of system hardware in the event of a physical catastrophe. However, all system hardware essential to the operation of CHRIS is stored in one location. This creates the potential for an almost total loss of the system's ability to restore functions should a catastrophic event occur. IA found ETS mitigates the risk of data loss by performing nightly data backups. These backups are then transferred to an offsite location on a daily basis, allowing for the preservation of data. However, this provides no abatement of the financial loss and ramifications for the continuity of City operations should all CHRIS hardware be destroyed.

Recommendation 5: Establish, implement and test a Disaster Recovery Plan.

Department Response: Agree. Funding to update the ETS Data Center and implement a Disaster Recovery plan is budgeted in FY2017. Additionally, the City Manager's Office has initiated a citywide I.T. Standardization and Optimization initiative to evaluate all city I.T. personnel and improve the city's current technology service delivery model. As part of this effort, all of the city's data center infrastructures are being evaluated to determine the city's collective data center capacity and DR needs. A comprehensive citywide data center disaster recovery plan is targeted to be in place by the Q1 of FY2018.

Processes for granting and terminating CHRIS user accounts need strengthening.

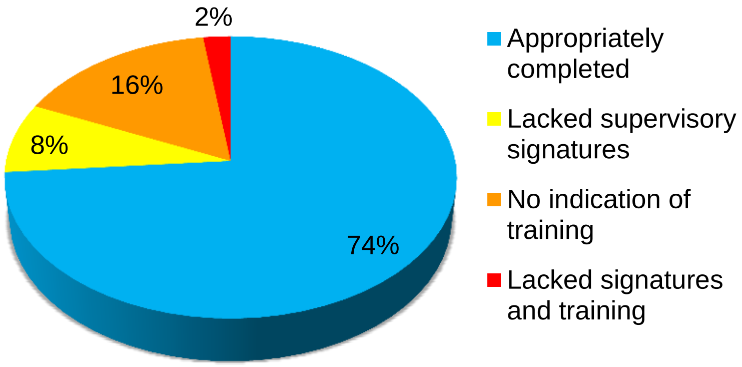
The CHRIS account creation and termination process is reliant upon a decentralized model that places the responsibility on individual's supervisors to ensure that CHRIS accounts are only assigned to active and appropriate personnel. The activation and termination of a CHRIS user account is initiated from the department in which the individual is employed. The process begins with the submittal of an *Application for CHRIS Access* form to ETS, complete with information on the employee and approval from the employee's direct supervisor. The form is then routed to the supervisor of the functional area for which access is being requested in order to obtain the appropriate approval. The CHRIS functional designations include Payroll, Training, HR, Budget, and Health and Safety and allow the user to access other employees' information. Privileges assigned to an account allow the user to either view information or view and edit information. Any designation that allows for the editing of information requires the completion of a training course. Upon training completion, the date of training is indicated on the form. The termination process is also initiated by the department and requires the relevant department to contact ETS to remove access.

IA reviewed all CHRIS access applications from January 2014 through July 2016 for users whose designation would allow the user to access other employees' information. This resulted in a sample of 137 CHRIS applications. Of this total, IA found a total of 36 forms (26%) forms with documentation issues. Eleven forms (8%) did not possess all of the required supervisory signatures. All 11 of these forms were missing approval from the functional area for which access was requested or were missing the final approval from ETS. No forms were missing

[1] The Disaster Recovery and Business Continuity chapter within the City of Cincinnati Information Security Policy states, "The department is responsible for creating and implementing a disaster recovery strategy…Disaster recovery and business continuity strategies, plans, and processes are to be tested at least yearly by the department."

approval from their direct supervisor approving their initial request for access. Twenty-two forms (16%) did not include the date of the required training. Three forms (2%) lacked both required signatures and training dates. One of these forms was missing the approval of the individual's direct supervisor. A graphical depiction of the above is presented in Figure 1 below.

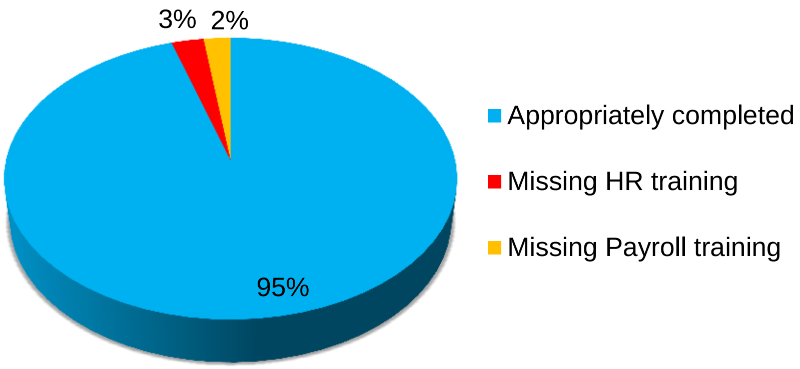
Figure 1 - CHRIS Access Applications



Although the lack of documentation creates obstacles for verification of appropriate access by a third-party, the risk associated with this is generally low. The absence of approval from the given functional areas does not suggest the need for access is not warranted given that the majority of forms possessed approval from their direct supervisor. The implication of missing training verification is also not extremely detrimental: most users have completed the required training, it is simply not documented. In fact, a master list is maintained within the CHRIS system that updates when a user attends the training course required by their access level.

Given the low risk of the previously mentioned documentation issues, IA sought to investigate the prevalence with which accounts that required training were not documented on the master list of training attendees. With assistance from CHRIS personnel, all accounts that had the ability to edit information in either the HR or Payroll functional areas were cross referenced with the list of individuals who had attended the required training. Of these 230 accounts, 11 accounts (5%) were granted access without the required training. These included six accounts (3%) with HR update capabilities and five accounts (2%) with payroll update capabilities. This is visually depicted in Figure 2 below. The complete absence of training poses a greater degree of risk to the system than the lack of training documentation. Users who have not been exposed to the necessary security procedures are more likely to unintentionally compromise system security.

Figure 2 - Training for HR and Payroll Accounts with Update Capabilities



IA also reviewed the employment status of all CHRIS users with privileges allowing for the accessing of other employees' information. As of July, 2016, there were a total of 334 CHRIS accounts with these assigned privileges. IA found four accounts (1%) assigned to individuals who were not City employees. Of these four accounts, two belonged to former City employees currently hired as contractors and two belonged to former interns.

The ability of third-party individuals to access City employee's PII is a cause for concern as ETS does not require departments to conduct background checks on third-parties. The accounts assigned to the former interns merit additional concern: their accounts were active (as of August 2016), in spite of the fact that they had been separated from the City since December 2015. Active accounts belonging to terminated individuals increases the risk of unauthorized use of any PII contained within the CHRIS system. Terminated individuals with active CHRIS accounts are the result of a breakdown of internal controls that can occur when a decentralized system is in place. In 2014, ETS conducted a citywide sweep of CHRIS accounts to eliminate those belonging to terminated individuals. However, this has not occurred since.

Recommendation 6: Ensure access is granted to appropriate personnel by generating an account only after all required signatures are received.

Department Response: Agree. In the past, the ETS CHRIS team received directives from department heads and other VIPs to provide immediate CHRIS access to certain individuals, bypassing the established process and required signatures. This practice is no longer in use. Accounts will only be created if the proper authorizations are present.

Recommendation 7: Ensure all individuals with CHRIS accounts receive the required training before access is granted.

Department Response: Agree. CHRIS training is conducted by the functional areas – they are responsible for ensuring new CHRIS users have received the proper training. Moving forward, the ETS CHRIS team will not enable any new CHRIS accounts unless the functional areas have signed off that the employee has received adequate training.

Recommendation 8: Strengthen internal controls to ensure timely termination of accounts corresponding to an individual who no longer requires access. At a minimum, ETS should contact all City departments on an annual basis for a complete list of all separated employees and third-party entities.

Department Response: Agree. ETS will begin running a monthly termination report to identify and remove access for anyone no longer employed by the City. In addition, ETS has implemented changes to the Application for CHRIS Access form to record the date and individual who removed the employee's access. We're also planning to scan each application/termination and attached the electronic image of the form to the employee's CHRIS account. This will preserve a permanent copy of the access/termination form.

Recommendation 9: Require departments to conduct background checks for any third-parties who are assigned a CHRIS account designation that allows access to PII.

Department Response: Agree. ETS believes this requirement should originate from the Human Resources Department since it relates to personnel policy.

Maintenance of records is not in compliance with City policies and CHRIS' record retention policies need to be updated.

Upon an individual's separation from the City, their corresponding CHRIS account is deleted from the system and their corresponding physical application for access is discarded. The former user's only remaining record is the date of completion of a training course, if required by their user status. This creates difficulties when attempting to review individuals with prior access capabilities and inhibits the ability of identifying user accounts that may have engaged in unauthorized activities.

According to the City's HR policy on record retention,[2] all official records are to be maintained for inspection and record retention schedules are to be updated as policies change. There have been no updates to ETS' record retention policies since 2004 and it is unclear if the current practice of discarding of applications is in compliance with the City's and ETS' policies.

Recommendation 10: Halt the destruction of all terminated users' CHRIS applications until the appropriate record retention policies can be identified.

Department Response: Agree. All application forms will be maintained even after the user's access has been terminated. See department response to recommendation 8 above.

Recommendation 11: Ensure all record retention policies are up to date and reflect the current department practices.

Department Response: Agree. ETS' records retention schedule is updated when necessitated due to a change in policy. ETS will review and update its retention schedule as needed to align with current policy by the end of the 2016 calendar year.

[2] City of Cincinnati Human Resources Policies and Procedures Records Retention Policy § 2.9 states, "records will be organized and maintained so that they are readily available for inspection and copying and the record retention schedules are updated regularly and posted prominently on the City's website."

Lenient password policies increase the likelihood of unauthorized access through the login portal.

Stringent password controls reduce the likelihood of unauthorized access through the primary port of access. All components of CHRIS' current password policy are in direct violation of City policy[3] and do not adequately restrict access to the system. CHRIS password controls allow passwords to remain valid for 180 days for all accounts. However, City policy requires administrator passwords expire after 42 days and user passwords expire after 90 days. CHRIS Password Controls also have no syntax requirements in spite of the City's policies requiring passwords contain both upper and lower cases, numbers and special characters. The system's automatic account lockout is also out of compliance; the CHRIS policy locks out users after five failed attempts to access the system while the City's policies require automatic account lockout to occur after three failed attempts to access the system. Finally, the length of time for a user's account to be automatically purged due to inactivity is 500 days. The National Institute of Standards and Technology[4] recommends user profiles be deleted after 90 days of inactivity.

Recommendation 12: Align CHRIS Password Controls with the City's password policies as stated in the ISP.

Department Response: Agree. The CHRIS password requirements will be reviewed by the CHRIS team to determine the impact of aligning them with the city's password policy. A review will be prepared for the new ISO with the objective of mitigating the identified login and password risks and conforming them with the city's Information Security policy when updated. It's anticipated the new ISO will complete the security policy review and update by the end of Q2 2017.

Authorization forms granting access to the City's hardware or allowing an individual to bypass the City's firewall are occasionally incomplete.

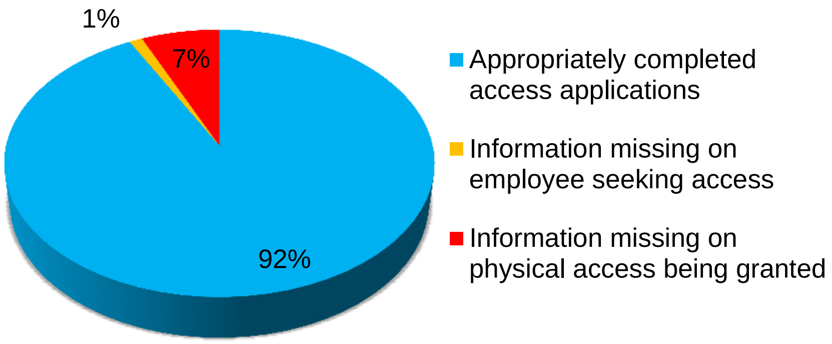
Separate forms are used to request physical access to the Data Center, the location of the majority of the City's hardware, and to grant physical possession of tokens that allow an individual to remotely bypass the City's firewall. IA reviewed a subset of both forms to ensure they were properly completed and maintained.

IA reviewed all *Data Center Physical Access* forms that had a completion date of 2008 or later. Since 2008, 90 individuals have been granted access to the Data Center upon the submission of an access form. Seven (8%) of these forms were missing information; one form (1%) was missing information regarding the employee seeking access and six forms (7%) were missing information regarding the specifics about the physical access being granted. Figure 3, below, displays these results. Further, as of August, 2016, there were 43 individuals who had physical access to the Data Center. However, six individuals (14%) with Data Center access did not correspond with a form approving this access.

[3] See the Passwords chapter of the City's Information Security Policy.

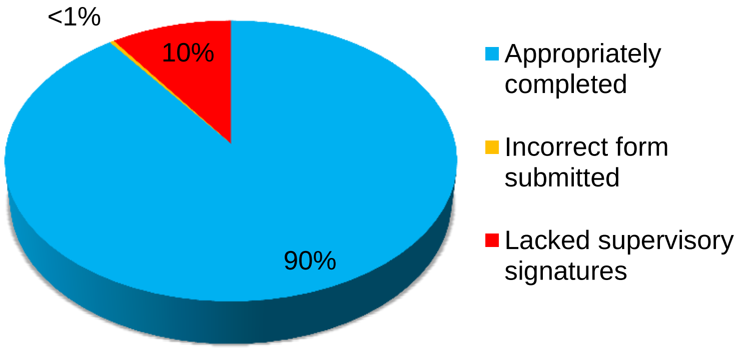
[4] Swanson, Marianne, and Barbara Guttman. *Generally accepted principles and practices for securing information technology systems*. National Institute of Standards and Technology, Technology Administration, US Department of Commerce, 1996.

Figure 3 - Data Center Physical Access Applications



Remote access is granted to designated employees and third-party entities based upon the need to access City information systems offsite. In order to grant remote access, ETS requires the employee seeking access to submit an application for remote access with the signatures of their direct supervisor and department director. IA reviewed 277 forms dated from January 2013 through July 2016 to ensure forms were complete before access was granted. IA found 28 forms (10%) with documentation inconsistencies or errors: 27 of these forms (10%) were lacking required signatures while one (0.4%) form was submitted using a *Business Partner Access Form* instead of the appropriate *Remote Access Form.* Figure 4, below, displays these results. In addition, there were 31 forms from the Law Department that lacked the signatures of a sponsoring employee, the ISO and the ETS Director. However, all 31 forms had the same date requested for initial access and appeared to be photo-copies of the same initial application, leading IA to assume that there was some sort of verbal discussion surrounding their submittal and approval.

Figure 4 - Remote Access Applications



The lack of consistency in approving both form types and the missing documentation of access approval to the City's hardware creates uncertainty when attempting to determine if individuals have a verified need for either access type. This can also allow for confusion when it is necessary to identify individuals with a given access level.

Recommendation 13: Exercise consistent documentation procedures in granting access to the Data Center and the physical possession of remote access tokens.

Department Response: Agree. The current process for granting access to the ETS data center will be reviewed collaboratively by the ETS Director, the CHRIS team, the Data Center team, and the new ISO. The process will be updated to insure that all access forms are completed and stored as needed. This process will be completed by the end of Q1 2017.

Third-party entities are in possession of remote access tokens.

Remote Access tokens are physical hardware that allow a user to bypass the City's firewall when not on City property. While remote access can be granted to third-parties through a sponsoring City employee, the ISP explicitly prohibits the issuing or possession of remote access tokens to such non-City employees.[5] Through interviews, it was revealed that third-parties are routinely granted physical possession of remote access tokens. Furthermore, records designating which tokens are assigned to City employees versus non-City employees are not maintained. Although remote access may be warranted for non-City employees, the granting of physical tokens to non-City employees removes an additional layer of oversight since tokens allow for unlimited remote access capabilities.

Recommendation 14: Collect all remote access tokens currently in the possession of non-City employees and halt the practice of distributing tokens to third-party entities.

Department Response: Agree. This finding is a direct result of the city's outdated security policy. The City's current remote access solution and process for approving, denying, and controlling remote access to the city's business network needs to be improved for both city employees and third parties. The city has a number of vendor supported systems that require remote access for their support providers. The current remote access policy does not satisfy this city business need. This finding will be addressed during the update of the security policy and should be completed by end of Q2 2017.

Group accounts exist where multiple individuals are able to bypass the City's firewall using the same login credentials.

City policy prohibits remote access accounts be assigned to more than one individual.[6] However, IA found group accounts exist for consultants where multiple individuals are able to bypass the City's firewall using the same login credentials. The existence of group accounts implies CHRIS is unable to determine the individual utilizing the account accessing the remote access system if necessary.

Recommendation 15: Create additional accounts with unique credentials for individuals who are currently registered to group accounts and immediately halt the practice of issuing the same user account to multiple individuals.

[5] The Remote Access chapter within the City of Cincinnati Information Security Policy states, "Non-city entities are not to be given a remote access token. The token will reside with the supporting City of Cincinnati entity..."

[6] The Remote Access chapter within the City of Cincinnati Information Security Policy states, "Tokens and remote access must not be shared by more than one person."

Department Response: Agree. This finding is a direct result of the city's outdated security policy. The City's current remote access solution and process for creating accounts to access the city's business network needs to be improved for both city employees and third parties. The city has a number of vendor supported systems that require remote access for their support providers. The current remote access policy does not satisfy this city business need. This finding will be addressed during the update of the security policy and should be completed by end of Q2 2017.

Annual reviews of users with remote access capabilities are not conducted.

City policy requires annual reviews of the list of individuals with remote access.[7] Through staff interviews, IA found ETS personnel had no knowledge of these annual reviews occurring. Without this annual review process, users may retain remote access to the system past the date of legitimate need for access. This issue was brought to the attention of the Acting ISO and is currently under review.

Recommendation 16: Conduct annual reviews of the list of individuals with remote access capabilities and verify their need is current.

Department Response: Agree. The ETS security team and data center team will initiate an audit of all users with remote access. This audit will re-occur annually as part of the updated information security policy.

[7] The Remote Access chapter within the City of Cincinnati Information Security Policy states, "The ETS Director, or designee, and the ISO, or designee, will perform, at minimum, annual reviews of person(s) with remote access privileges to the MAN."

III. Conclusion

The Cincinnati Human Resource Information System (CHRIS) provides essential human resource services to all City employees and facilitates the accessing of information. The audit revealed several opportunities for improvement over the internal controls surrounding CHRIS.

Outdated and obsolete policies, a lack of compliance, inadequate oversight and low staffing levels have led to an increased risk for unauthorized system access. It is imperative that ETS create and enforce a new ISP that specifically addresses CHRIS and contains a Disaster Recovery Plan. Additionally, IA recommends reviewing staffing levels to determine if they are appropriate for the system’s needs; apply consistent standards to documenting processes granting any degree of access and ceasing all current practices in violation of City policies. These changes will facilitate verification of active users, provide guidance as to required operations and reduce the risk generated by unacceptable practices.

IV. ETS Department Response

Recommendation 1: Update the ISP to reflect current operating procedures and industry best practices. This includes creating policies specific to maintaining the integrity and confidentiality of employees' PII within CHRIS. Only practices that the City has intent of enforcing and utilizing and that have been determined to add value to IT operations should be incorporated.

Department Response: Agree. ETS has been unable to permanently fill the Information Security Officer and Security Analyst FTE positions since 2015 due to budget constraints. As a result, the City's Information Security Policy has not been updated since 2005 and is out of date. In the ETS FY17 budget, funding for the ISO and 2 Security Analysts has been restored to the operating budget. The ISO and Security Analyst positions will be filled in Q4 of FY2017. Updating the Security Policy will be an immediate deliverable for the new ISO. The CHRIS technical team and City HR will be consulted to insure that onboarding, off-boarding, and CHRIS information security needs are captured and updated in the refreshed security policy.

Recommendation 2: Consult with HR to determine the appropriate staffing level that will allow for improved system maintenance and ensure the allocation of duties amongst personnel aligns with current IT standard practices.

Department Response: Agree. The CHRIS technical team currently consist of an I.T. Assistant Manager, 2 full-time Computer Systems Analysts, and a part-time Computer Systems Analysts. ETS will evaluate the CHRIS system support requirements and determine if the current CHRIS team roles and responsibilities can be adjusted to allow duties to be segregated, staff to be cross trained, and a succession plan to be implemented to preserve institutional system knowledge due to possible retirements in upcoming years. An additional CSA FTE or professional services resource for the CHRIS team has been budgeted in FY2017.

Recommendation 3: Implement mitigating controls to ensure there is proper segregation of duties for the current staffing level.

Department Response: Agree. See department response to recommendation 2 above.

Recommendation 4: Hire an individual who has the ability to fulfill the duties of the ISO position.

Department Response: Agree. See department response to recommendation 1 above.

Recommendation 5: Establish, implement and test a Disaster Recovery Plan.

Department Response: Agree. Funding to update the ETS Data Center and implement a Disaster Recovery plan is budgeted in FY2017. Additionally, the City Manager's Office has initiated a citywide I.T. Standardization and Optimization initiative to evaluate all city I.T. personnel and improve the city's current technology service delivery model. As part of this effort, all of the city's data center infrastructures are being evaluated to determine the city's collective data center capacity and DR needs. A comprehensive citywide data center disaster recovery plan is targeted to be in place by the Q1 of FY2018.

Recommendation 6: Ensure access is granted to appropriate personnel by generating an account only after all required signatures are received.

Department Response: Agree. In the past, the ETS CHRIS team received directives from department heads and other VIPs to provide immediate CHRIS access to certain individuals, bypassing the established process and required signatures. This practice is no longer in use. Accounts will only be created if the proper authorizations are present.

Recommendation 7: Ensure all individuals with CHRIS accounts receive the required training before access is granted.

Department Response: Agree. CHRIS training is conducted by the functional areas – they are responsible for ensuring new CHRIS users have received the proper training. Moving forward, the ETS CHRIS team will not enable any new CHRIS accounts unless the functional areas have signed off that the employee has received adequate training.

Recommendation 8: Strengthen internal controls to ensure timely termination of accounts corresponding to an individual who no longer requires access. At a minimum, ETS should contact all City departments on an annual basis for a complete list of all separated employees and third-party entities.

Department Response: Agree. ETS will begin running a monthly termination report to identify and remove access for anyone no longer employed by the City. In addition, ETS has implemented changes to the Application for CHRIS Access form to record the date and individual who removed the employee's access. We're also planning to scan each application/termination and attached the electronic image of the form to the employee's CHRIS account. This will preserve a permanent copy of the access/termination form.

Recommendation 9: Require departments to conduct background checks for any third-parties who are assigned a CHRIS account designation that allows access to PII.

Department Response: Agree. ETS believes this requirement should originate from the Human Resources Department since it relates to personnel policy.

Recommendation 10: Halt the destruction of all terminated users' CHRIS applications until the appropriate record retention policies can be identified.

Department Response: Agree. All application forms will be maintained even after the user's access has been terminated. See department response to recommendation 8 above.

Recommendation 11: Ensure all record retention policies are up to date and reflect the current department practices.

Department Response: Agree. ETS' records retention schedule is updated when necessitated due to a change in policy. ETS will review and update its retention schedule as needed to align with current policy by the end of the 2016 calendar year.

Recommendation 12: Align CHRIS Password Controls with the City's password policies as stated in the ISP.

Department Response: Agree. The CHRIS password requirements will be reviewed by the CHRIS team to determine the impact of aligning them with the city's password policy. A review will be prepared for the new ISO with the objective of mitigating the identified login and password risks and conforming them with the city's Information Security policy when updated. It's anticipated the new ISO will complete the security policy review and update by the end of Q2 2017.

Recommendation 13: Exercise consistent documentation procedures in granting access to the Data Center and the physical possession of remote access tokens.

Department Response: Agree. The current process for granting access to the ETS data center will be reviewed collaboratively by the ETS Director, the CHRIS team, the Data Center team, and the new ISO. The process will be updated to insure that all access forms are completed and stored as needed. This process will be completed by the end of Q1 2017.

Recommendation 14: Collect all remote access tokens currently in the possession of non-City employees and halt the practice of distributing tokens to third-party entities.

Department Response: Agree. This finding is a direct result of the city's outdated security policy. The City's current remote access solution and process for approving, denying, and controlling remote access to the city's business network needs to be improved for both city employees and third parties. The city has a number of vendor supported systems that require remote access for their support providers. The current remote access policy does not satisfy this city business need. This finding will be addressed during the update of the security policy and should be completed by end of Q2 2017.

Recommendation 15: Create additional accounts with unique credentials for individuals who are currently registered to group accounts and immediately halt the practice of issuing the same user account to multiple individuals.

Department Response: Agree. This finding is a direct result of the city's outdated security policy. The City's current remote access solution and process for creating accounts to access the city's business network needs to be improved for both city employees and third parties. The city has a number of vendor supported systems that require remote access for their support providers. The current remote access policy does not satisfy this city business need. This finding will be addressed during the update of the security policy and should be completed by end of Q2 2017.

Recommendation 16: Conduct annual reviews of the list of individuals with remote access capabilities and verify their need is current.

Department Response: Agree. The ETS security team and data center team will initiate an audit of all users with remote access. This audit will re-occur annually as part of the updated information security policy.