TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Updating Computer Room and Tape Library Physical Access Controls at the Computing Centers Will Significantly Improve Security

September 29, 2016

Reference Number: 2016-20-093

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

UPDATING COMPUTER ROOM AND TAPE LIBRARY PHYSICAL ACCESS CONTROLS AT THE COMPUTING CENTERS WILL SIGNIFICANTLY IMPROVE SECURITY

Highlights

Final Report issued on September 29, 2016

Highlights of Reference Number: 2016-20-093 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

Computer rooms and tape libraries house critical IRS systems and data that reside on mainframes, servers, and other information technology equipment as well as back-up tapes for operations. These systems are essential to the operations of the IRS. Unauthorized access could result in the theft of equipment and taxpayer information and disruption of service.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our statutory requirement to annually review the adequacy and security of IRS technology. The overall objective was to assess the controls in place to restrict access to computer rooms and tape libraries, and to prevent and detect unauthorized accesses to those resources.

WHAT TIGTA FOUND

TIGTA determined that computer room and tape library perimeter security needs to be updated. Two-factor authentication was not being used for one of the data center locations, and door testing was not being performed after changes to or implementation of the door groups in the enterprise Physical Access Control System (ePACS). As a result, general access was allowed into the restricted computer rooms. Also, surveillance equipment was either outdated or did not exist, which limited the IRS's ability to monitor its critical infrastructure.

TIGTA also determined that the continued use of temporary badges as a form of identification presents security concerns because these badges do not provide specific employee information. Also, the IRS uses a manual and visual process to identify visitors, increasing the risk that an unauthorized individual could gain access. Authenticating individuals by their Personal Identity Verification cards reduces that risk because the card authenticates the individual entering the room.

Lastly, TIGTA determined that automating access monitoring to the computer rooms and tape libraries will increase efficiency and security.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief, Agency-Wide Shared Services, periodically test card readers to ensure correct association with the door group in the ePACS, implement compliant two-factor authentication, update security surveillance equipment, align policy for temporary badges with Federal policy, add unique identifiers to the ePACS, and maintain and ensure consistency in the use of *Limited Area Registers*. TIGTA also recommended that the Chief Information Officer update policies and/or procedures to require the use of a secure automated system to authorize and approve access, ensure sufficient oversight and coordination between the Enterprise Computing Center Project Response Incident and Management office and tape library management, review monthly ePACS reports, and discontinue Level 1 and Level 2 designations based on frequency of access.

The IRS agreed with six recommendations, partially agreed with two recommendations on repairing cameras and updating procedures for monthly reconciliation of logs, and disagreed with the five recommendations on updating policies for cameras and monitoring physical intrusion alarms, temporary badges, controlling of access into computer rooms, the need to remove Levels of access, and business need for access.

TIGTA maintains that the IRS should take additional corrective actions with respect to both of the partially agreed recommendations and the five disagreed recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 29, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Updating Computer Room and Tape Library Physical Access Controls at the Computing Centers Will Significantly Improve Security (Audit # 201620010)

This report presents the results of our review to assess the controls in place to restrict access to computer rooms and tape libraries, and to prevent and detect unauthorized accesses to those resources. This audit is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Internal Revenue Service (IRS) Employees. This audit was also part of our statutory requirement to annually review the adequacy and security of IRS technology.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

AWSS	Agency-Wide Shared Services
CCTV	Closed Circuit Television
DVR	Digital Video Recorder
ECC	Enterprise Computing Center
EOps	Enterprise Operations
ePACS	Enterprise Physical Access Control System
FIPS	Federal Information Processing Standard
HSPD-12	Homeland Security Presidential Directive 12
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
PDF	Portable Document Format
PIN	Personal Identification Number
PIV	Personal Identity Verification
PRIMO	Project Response Incident and Management Office
SOP	Standard Operating Procedure
TIGTA	Treasury Inspector General for Tax Administration

Background

Homeland Security Presidential Directive-12 (HSPD-12),[1] *Policy for a Common Identification Standard for Federal Employees and Contractors*, issued in August 2004, mandated the establishment of a Governmentwide standard for identity credentials to improve physical security in federally controlled facilities. HSPD-12 required all Government employees and contractors be issued a new identity card based on Federal Information Processing Standard (FIPS) 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*.[2] HSPD-12 explicitly requires the use of HSPD-12 PIV cards "in gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems."

The Internal Revenue Service's (IRS) two main data centers, also known as its Enterprise Computing Centers (ECC), are located in Memphis, Tennessee, and Martinsburg, West Virginia, and are both Facility Security Level 5 areas as defined by the Department of Homeland Security.[3] Facility Security Level 5 is the highest level that can be assigned to a Government facility and is based on criticality and both its attractiveness as a target and the consequences of an event. The ECCs house some of the most critical systems and data for the IRS. For example, the computer rooms contain the mainframes that run the Master File, which contains sensitive taxpayer information, as well as servers and other computer equipment for operations, and tape libraries which store critical system operations and back-ups.

Access to all computer rooms and tape libraries at the ECCs are managed by the Information Technology's (IT) Enterprise Operations (EOps) organization. The IRS uses the enterprise Physical Access Control System (ePACS) to control access to and within the facility. Card readers are placed at doors for users to swipe their HSPD-12 PIV cards and, for some areas, enter a personal identification number (PIN) for two-factor authentication. Because the areas within a facility may be accessible via different access points and may not require the same level of authentication to access, the PIV authentication mechanisms selected for the area should be consistent and represent the overall security level of the protected area. For example, a single facility may need multiple authentication mechanisms. The National Institute of Standards and Technology (NIST) Draft Special Publication 800-116, Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*,[4] lays out the designations of "Controlled," "Limited," or "Exclusion" that should be applied to protected areas. The IRS uses

[1] See Appendix IV of the glossary of terms.
[2] U.S. Department of Commerce, Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*, (Aug. 2013).
[3] U.S. Department of Homeland Security, Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, 1st edition (Aug. 2013).
[4] U.S. Department of Commerce, NIST Special Publication 800-116, Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*, (Dec. 2015).

the "Restricted" designation in lieu of "Limited." Figure 1 defines the number of authentication factors required for the different security areas.

Figure 1: Authentication Required for Designated Security Areas

Security Areas	Number of Authentication Factors Required
Controlled	**1**
Limited (IRS - Restricted)	**2**
Exclusion	**3**

Source: NIST Draft Special Publication 800-116, Revision 1.

ECC-Martinsburg and ECC-Memphis computer rooms are both designated as "Limited" areas. The ECC-Memphis tape library is designated as a "Controlled" room within the "Limited" computer room because it is co-located; however, the ECC-Martinsburg tape library is designated as "Limited" because it is accessible outside of the "Limited" computer room. The number of authentication factors increases the reliability as to someone's identity. That is why more factors are needed as the security area gets more restrictive.

The Agency-Wide Shared Services (AWSS) organization is responsible for monitoring the physical access of those who enter the computer rooms and tape libraries and for using the ePACS to capture all transactions of individuals entering the restricted computer rooms and tape libraries. AWSS organization personnel work with EOps organization personnel to ensure that only those individuals authorized by the EOps organization to enter the computer rooms and tape libraries have the proper access assigned to their HSPD-12 PIV cards. EOps organization personnel also notify AWSS organization personnel when access should be removed.

IRS policies require that computer rooms and tape libraries be secured and monitored 24 hours a day, 7 days a week. Access to computer rooms and tape libraries is determined by the EOps organization and should be restricted to employees with authorized entry and is granted on a site-by-site, case-by-case basis, using two levels of access determined by frequency (of accessing the rooms). Level 1 access is intended for those individuals who require frequent and continuous access to computer rooms, such as system administrators, database administrators, computer operators, or computer system analysts, to perform their duties as determined by the approving official. Level 2 access will be approved for individuals who have a business need to enter the computer room or tape library on an occasional basis.

This review was performed at the ECCs located in Memphis, Tennessee, and Martinsburg, West Virginia, within the IT EOps organization and the AWSS organization's Physical Security office during the period January through June 2016. We conducted this performance audit 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions

based on our audit objective. Due to time constraints, the scope of this review was limited and did not take into consideration the backgrounds of those entering the computer rooms and tape libraries. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Computer Room and Tape Library Perimeter Security Needs Improvement

The ePACS card readers are used at the doors of the computer rooms and tape libraries to allow access to those who are authorized to enter. Every time someone swipes a HSPD-12 PIV card and enters a PIN, the ePACS records the transaction. One of the functions of the ePACS application is to verify the identity of the cardholder. The confidence in the cardholder's identity increases with the number of factors used to authenticate the HSPD-12 PIV card.

The ePACS door tests should be conducted

We tested card readers at the ECC-Memphis and the ECC-Martinsburg to ensure that they were accurately capturing transactions on the ePACS when used. Doors within the facilities are labeled, and the ePACS card readers capture the specific door that is being accessed. This labeling allows doors associated with a particular room or area to be grouped within the ePACS. Individuals are allowed access by having the door groups assigned to their PIV card.

We reviewed the door groups to ensure that restricted door access was assigned to the correct groups and identified the following situations in either the ECC-Martinsburg or the ECC-Memphis locations where particular doors were not assigned to the correct door groups:

- The doors leading from the dock into the main computer room allowed any person with general access capability to enter the computer room.
- The doors in the Shipping Door group allowed access to both the main computer room and tape library. These doors did not require two-factor authentication and allowed access to a restricted area.
- The door leading to the tape library was in the main computer room door group allowing anyone with access to the computer room to have access to the tape library.
- Some doors were labeled incorrectly for entry and exit situations.

The AWSS organization's Physical Security office corrected these situations immediately after being informed. However, the door groups should have been tested after implementing ePACS card readers or making specific changes to the groups. This testing should also include the testing of restricted door groups with different cards on an annual basis to ensure that the doors only allow the authorized access.

During our site walkthrough and discussion with local IRS employees, we were informed by ECC-Martinsburg tape library personnel about a prior instance in which an unknown individual gained access to the tape library and was observed wandering in the area without a proper identification badge. An employee challenged this person who indicated that he or she was lost and needed assistance on how to exit the area, which we interpreted as this person did not belong in the area and needed to be escorted out. Management could not explain how the individual gained access to the restricted area. The employee could not specify the exact date of the incident, so we could not further evaluate the incident and corroborate what occurred. However, we believe this apparent security breach illustrates what could happen when doors are not labeled correctly.

When doors are improperly included in the wrong door groups, it allows people to gain unauthorized access to restricted or controlled areas. In this case, it was troubling because the restricted computer rooms and tape libraries house the critical IRS systems, such as mainframes, servers, and other information technology equipment and systems, as well as the back-up tapes for operations. These systems are essential to the operations of the IRS. Unauthorized access could result in theft of data and equipment, destruction of property, and willful or accidental disruption of operations.

Two-factor authentication needs to be implemented at the ECC-Memphis

According to FIPS 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*,[5] the PIV card is the primary component of the PIV system. The holder uses the PIV card for authentication to various physical and logical resources. Card readers are located at access points for controlled resources where a cardholder may wish to gain access (physical and logical) by using the PIV card. The reader communicates with the PIV card to retrieve the appropriate information, located in the card's memory, to relay it to the access control systems for granting or denying access. PIN input devices can be used along with card readers when a higher level of authentication assurance is required.

The Internal Revenue Manual (IRM) defines a limited area to which access is limited to authorized personnel only. For a limited area, the IRM also requires two-factor authentication.

Currently, the ECC-Memphis only has one-factor authentication as defined by NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*,[6] for access to the computer rooms. Possession of a valid PIV card as evidenced by visual inspection of the card, reading a signed object from the card, or performing challenge/response authentication with the card, provides one-factor authentication. At the ECC-Memphis location, employees with either Level 1 or Level 2 access are required to swipe

[5] U.S. Department of Commerce, Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*, (Aug. 2013).
[6] U.S. Department of Commerce, NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, (Nov. 2008).

their HSPD-12 PIV card to gain access. Although a security guard visually checks the person's PIV card at the entrance of the computer rooms, this process does not constitute two-factor authentication as defined by FIPS 201.

Visual authentication entails inspection of the topographical features on the front and back of the PIV card. The security guard is responsible for checking the authenticity of the PIV card, which includes comparing the cardholder's facial features with the picture on the card, checking the expiration date printed on the card, verifying the correctness of other data elements printed on the card, and visually verifying the security features on the card. The effectiveness of this mechanism depends on the training, skill, and diligence of the guard. For example, a guard would need to match the face in spite of changes in physical appearance, *e.g.*, presence of a beard, mustache, eyeglasses, or different hair coloring or style. Counterfeit identification cards can pass visual inspections. Today's digital scanners, printers, and image editing software have made identity counterfeiting easier. Moreover, the visual verification of security features does not scale well across agencies because each agency may implement different security features. For these reasons, FIPS 201 has downgraded this authentication mechanism to indicate that it provides "LITTLE or NO" confidence in the identity of the cardholder.

The following are considered two-factor authentications:

- Two factors – something you have, something you know.
- Two factors – something you have, something you are.

Two-factor authentication is when the cardholder must present the card (something you have) and either enter a PIN (something you know) or submit a fingerprint (something you are) to unlock the card in order to successfully authenticate.

A valid biometric from the card may be compared against a live scan. Biometric readers, especially those used at access points to Limited and Exclusion areas, should have a proven capability to accept live fingers and reject artificial fingers. During our walkthrough, we did not identify any biometric readers at the ECC-Memphis location. They were ePACS card readers where the person scanned his or her card and the readers were also capable of accepting a PIN.

In August 2013, FIPS 201 stated that biometric readers may be located at secure locations where a cardholder may want to gain access. These readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its comparison with a real-time biometric sample. The use of biometrics provides an additional factor of authentication ("something you are") and providing the card ("something you have") for cryptographic key-based authentication. This provides for a higher level of authentication assurance.

The AWSS organization disagreed and cited that the guard visually checking the individual's badge, along with swiping the badge in the card reader, constitutes two-factor authentication of the badge because the biometric data are on the card. However, according to FIPS 201, proper

two-factor authentication requires something you have and something you know or something you are, which would require a PIN number or biometric reading.

If a person's credentials or a temporary badge is lost or stolen, another person could gain access into the computer rooms and cause damage to the facility or hardware with the compromised credentials. Mere possession of a valid PIV card as evidenced by visual inspection of the card provides only one-factor authentication. However, if a PIN is also required for two-factor authentication, this may mitigate the vulnerability.

Surveillance equipment needs updating

The Department of the Treasury requires[7] its bureaus to:

- Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.
- Monitor physical intrusion alarms and surveillance equipment.
- Employ video surveillance of bureau-defined operational areas and retain video recordings for at least 90 days, if not otherwise defined in formal bureau policy.

In addition, the IRM states that Closed Circuit Television (CCTV) is very useful in physical security operations. One of the keys that affect the effectiveness of the CCTV is the maintenance of the system and equipment. The system normally consists of a television camera, camera control box, recorder, monitor, two-way communication system, and electrical circuitry. To ensure that the CCTV has an effective field of view, surveillance capabilities should be checked on a routine basis to assess equipment effectiveness and to identify obstructions and gaps in coverage. The CCTV is frequently used as an integral part of an intrusion detection system. This may be accomplished by:

- Using sensors to establish a secured area, which includes a time lapse digital video recorder (DVR) to complement the sensors.
- Placing cameras at critical locations to provide direct visual monitoring from a vantage point such as an on-site protection console.
- Using the CCTV on gates, doors, and other security areas not staffed continuously.

The IRM is outdated and lacks specificity concerning CCTV operations. As a result, during our walkthrough of each of the facilities, we observed the following concerns on the surveillance equipment.

- Camera Functionality.

[7] U.S. Department of the Treasury, TD P 85-01, Volume II, *Treasury Information Technology Security Program*, (June 2009).

- The ECC-Memphis does not have any camera or surveillance equipment in the computer rooms or tape library. If an incident occurs, they will be unable to identify the source of the problem.
- Neither location has a security camera system that is programmed to automatically back up live video recordings.
- At the ECC-Martinsburg, the auto pan/zoom capabilities for each location specific camera were disabled and no longer functioned, which was caused by a prior power outage. Although the ECC-Memphis location has 98 security cameras programmed to automatically pan/zoom on the activity when a security event occurs, 26 of the 98 security cameras are currently out of service or no longer functioning, which creates a strong degree of uncertainty on whether the functioning cameras will actually auto pan/zoom in when an alarm sounds. When a security incident occurs, the guards have to manually identify the appropriate camera and pan in on the event.

- Surveillance Recording Capabilities.
  - The five ECC-Martinsburg DVRs and six ECC-Memphis DVRs, specific to a range of monitors, collect data to their maximum capacity and automatically overwrite existing data for new recordings.
  - The DVRs in the ECC-Martinsburg are checked by the AWSS organization's Physical Security office personnel on a weekly basis for proper functioning and a DVR Log is maintained. The DVRs in the ECC-Memphis are checked daily by the vendor as part of its maintenance contract. The security officer does not maintain a DVR Log, and he or she only checks the camera footage for ad-hoc requests.
  - The ECC-Martinsburg has one spare DVR available, but there is no alarm to alert when an active DVR has failed. The ECC-Memphis has no spare DVRs available; however, an alarm sounds to alert the guards on the ePACS monitor when an active DVR has failed.
- Funding is a challenge to upgrade the surveillance equipment in both facilities. ECC-Martinsburg security management has obtained the following quotes to either upgrade or replace the CCTV monitoring system.
  - A basic upgrade at $9,402 plus $4,670 in labor costs.
  - A more comprehensive monitoring system upgrade at a base cost of $140,382 plus $23,035 in options.
  - A third proposal of $40,594 and an optional digital Network Video Recorder (replacing the DVRs) package for $58,962.

Management did not timely resolve the security camera auto/pan zoom issue and did not provide for automatic back-up of security recordings. Additionally, the security monitoring and recording system is outdated, subject to device failures or malfunction of the auto pan/zoom capabilities, and suffers from funding shortfalls which have prevented urgently needed repairs, replacements, and upgrades.

Without working security surveillance equipment, it is difficult or near impossible to determine who or what may be responsible if an accident or incident were to occur within the computer rooms or tape libraries. If an unauthorized person gains access into the rooms, they could wreak havoc on the IRS's critical infrastructure.

Recommendations

The Chief, AWSS, should:

Recommendation 1: Update the ePACS policy, specifically, the Physical Security Operations Guide and the ePACS Operation Manual, to require testing of the programming of impacted cards when a door group is established or modified, and annually to ensure that access is properly controlled to restricted or limited areas.

> ***Management's Response:*** The IRS agreed with this recommendation, stating that the Chief, AWSS, will update the ePACS Installation Checklist to require annual testing of the programming of impacted cards when a door group is established or modified to ensure that access is properly controlled to restricted or limited areas.

Recommendation 2: Implement a FIPS 201 compliant two-factor authentication for the computer rooms and tape library at the ECC-Memphis.

> ***Management's Response:*** The IRS agreed with this recommendation, stating that it plans to install readers that will require PIN authentication for computer rooms at the ECC-Memphis.

Recommendation 3: Repair or update security surveillance equipment and ensure that the automatic security camera pan functions properly at the perimeters of limited areas when an alarm is triggered.

> ***Management's Response:*** The IRS partially agreed with this recommendation, stating that camera repairs were completed in July 2016, but disagreed with updating the camera software to include automated panning, as this is above the current standard.
>
> ***Office of Audit Comment:*** Because the ECCs are designated as Facility Security Level 5, we believe time is of the essence in emergency situations and the guards should not be tasked with locating the correct camera where an alarm is triggered to manually pan and zoom onto the source of the alarm. We maintain that the automatic security camera pan function is necessary at both the ECC-Martinsburg and the ECC-Memphis

locations as this function was previously configured and can be again by the vendor support.

Recommendation 4: Update and include details in procedures and guidelines for monitoring physical intrusion alarms and surveillance equipment, such as security camera monitoring and recording; automatic back-up capabilities for the DVRs; and an alarm to alert security personnel when an active DVR has failed.

Management's Response: The IRS disagreed with this recommendation, stating that the IRS is compliant with the Interagency Security Committee's *Risk Management Process for Federal Facilities*, dated January 7, 2016, that requires the CCTV on limited access points, and TIGTA's recommendation is above the standard required for Federal facilities.

Office of Audit Comment: The IRS ECCs are designated as Facility Security Level 5 and house the IRS's critical infrastructure. As such, we continue to believe that the IRS needs to address the need for updates to the security surveillance equipment to enable automatic back-up of DVR recordings and an alarm when a DVR fails to function to promote the security and resilience of the Nation's critical infrastructure to physical threats.

Increased Security Concerns Remain With the Use of Temporary Badges

IRS policy from July 2009 states that the appropriate credentialing process is selected once the hiring decision is made. This determination is based on two major factors.

- Employment category (current or new employee/contractor).
- Appointment length (less than/greater than 180 days).

The ePACS Release 3 *Physical Security Operations Guide*, Version 3.1, states that Physical Access Cards are for employees and contractors who need short-term use only, *i.e.*, less than 180 days. Legacy cards will not have the features of SmartID cards. Legacy, or "PIV I," credentials are standard visitor badges and require no Federal Bureau of Investigation criminal check or background investigation. However, the IRS may determine that fingerprints, additional screening, and background checks are necessary based on the risk level of the work to be performed. The PIV card will eventually be used for access to IRS facilities and systems. Once this capability is established, employees and contractors will no longer require legacy cards.

IRM 10.2.4.2 further states that the authorized forms of identification media approved for use by IRS employees and contractors in the performance of official duties are as follows:

- Physical Access Card – designed for verification of identity and to provide physical access **only** into all IRS offices and issued to authorized contractors, seasonal employees, interns, and those IRS employees waiting for SmartID credentials.
- HSPD-12 SmartID card – designed for verification of identity and to provide physical access into all IRS offices and access to the IRS local area network, and is issued to all IRS employees and authorized contractors required by the HSPD-12.

However, this IRM is not clear as to whether the Physical Access Card is used for those employed less than 180 days.

During our walkthrough, we found the ePACS authenticates an individual with a PIV card at the entry points into the computer rooms and tape libraries. Temporary badges do not authenticate the individuals entering the computer rooms or tape libraries. The IRS relies upon the security guard's visual inspection of the photo identification that is presented in order to obtain a temporary badge. This method is not as secure as using a valid PIV to gain entry.

The NIST explains that, for a future ePACS maturity model Level 5, currently deployed non-PIV cards are not acceptable for authentication to any areas. That is, only the PIV card is an acceptable credential for Federal employees and contractors. According to the IRS, supplier solutions to meet NIST/FIPS compliance for Controlled or Limited access spaces just came into the vendor market in Fiscal Year 2015. Therefore, the use of temporary badges for visitors will be necessary for the indefinite future.

Individuals with Level 2 access use temporary badges to gain entry. The IRS stated that it established enhanced security controls for limited areas beyond the general access to facilities. These controls determine the frequency and type of access to the computer rooms and tape libraries that individuals need. For example, if a person needs to access a computer room or tape library infrequently, they are assigned a Level 2 access. For Level 2 access, the person checks in at the guard station and signs the Form 5421, *Restricted Area Register*, to obtain a temporary badge. If he or she currently has a PIV card, he or she retains it and is also issued a temporary badge at the guard station. If he or she does not have a PIV card, he or she swaps a photo identification, such as a valid driver's license, for a temporary badge to gain access, which is returned when he or she leaves the facility. The only verification of the photo identification or PIV card is the security guard's observation.

We determined that, in Calendar Year 2015, a temporary badge was used 7,848 times at the ECC-Martinsburg and 17,138 times at the ECC-Memphis to gain access to computer rooms.

Contractors employed more than six months should have restricted access assigned to their HSPD-12 PIV cards

The Office of Management and Budget[8] clarifies the eligibility requirements for a PIV card and defines temporary employees and contractors as those individuals employed for six months or less. These individuals are not required to receive an HSPD-12 PIV card, and agencies are permitted to issue temporary non-HSPD-12 PIV cards to these individuals. Although the IRS may have assigned a PIV card to contractors employed for more than six months, the IRS is still issuing them a temporary badge to access the limited area based on its enhanced security control for Level 2 access.

To determine whether Level 2 contractors should have been issued a PIV card, we reviewed a judgmental sample[9] of seven contractors from the ECC-Martinsburg and seven contractors from the ECC-Memphis locations who were identified from the *Restricted Area Registers* to determine if they were employed more than six months. The *Restricted Area Register* is currently used to document visitor information or contractor information for those who need a particular temporary badge to gain access to the computer rooms and tape libraries. We determined that six of the seven contractors in the ECC-Martinsburg and five of the seven contractors in the ECC-Memphis worked more than the six-month requirement for a temporary badge. Figure 2 shows the length of employment for contractors at each location.

Figure 2: Contractors Employed For More Than Six Months

Location	Number of Contractors	Length of Employment
ECC-Martinsburg	4 of 7	18 months
ECC-Martinsburg	2 of 7	12 months
ECC-Memphis	3 of 7	18 months
ECC-Memphis	2 of 7	12 months

Source: Treasury Inspector General for Tax Administration (TIGTA) analysis of the IRS's Restricted Area Register data.

The EOps organization had established policy that Level 2 access is intended for individuals who require computer room access on an occasional basis. Any admittance requires signing in at the guard station and acquiring a temporary badge.

However, this control may not be consistent with HSPD-12 guidelines. HSPD-12 explicitly requires the use of HSPD-12 PIV cards "in gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information systems." HSPD-12 attempts to

[8] Office of Management and Budget, M-05-24, *Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 2005).
[9] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

reduce the number of temporary badges by requiring that a person be issued a PIV card to be used to gain physical access when employed more than six months. We believe these 11 contractors should have received a HSPD-12 PIV card with the appropriate limited area access assigned to the card. The PIV card authenticates the person accessing the limited area where the temporary badge does not. Moreover, using a completely different card for accessing the limited area defeats the purpose of HSPD-12 and goes against the IRM policy for using the PIV card to gain physical access into all IRS offices.

Without proper authentication of the person entering the limited areas, there is an increased risk that the person may not be authorized to access the restricted area. Using a temporary badge does not authenticate the person entering the Limited space.

Badge numbers should be identified in ePACS transaction reports

One of the purposes of the ePACS is to record transactional information on individuals who actually enter the building, computer rooms, and/or tape libraries using their HSPD-12 PIV card. For individuals who use temporary badges, the ePACS transaction report will capture the type of badge information, such as temporary or visitor, Federal or non-Federal, and the accessible area. However, it will not capture information specific to the individual such as the name, employee status, and expiration date, all of which are critical in associating the individual to the use of the temporary badge. Therefore, the information captured in the ePACS transactional report cannot be easily used to make a one-to-one match with the person who was issued the temporary badge to gain access into the computer rooms and tape libraries. The current process to verify the identity requires manually matching the temporary badge number back to the *Restricted Area Register*. This process is a time consuming, two-step manual process that we believe should be automated to accurately capture the visitor's information. The temporary badge number is not in the description field on the transaction reports. A person must manually go back to the Enrollment Manager portion of the ePACS and research the badge number. Then the badge number must be matched back to the *Restricted Area Register* at the guard station to identify the person who was issued the badge.

The description field within the ePACS is usually populated with a person's name from the Enrollment Manager for a PIV card. When a person registers a PIV card at the current facility, the information is input into the Enrollment Manager portion of the ePACS. The credentialing specialist ensures that the information is correct. The following fields should be populated for the person's profile in the ePACS:

- Name.
- PIV Card Number.
- Expiration Date.
- Employee Status.

- Standard Employee Identifier.
- Expire Credentials Field.

The IRS stated that the Enrollment Manager portion of the ePACS also captures the badge number for temporary badges.

We reviewed a download of ePACS data that included all transactions recorded by the ePACS from January 2014 through January 2016. We separated the transactions by event codes for both accesses granted and denied. From a judgmental sample[10] of 40 temporary badge accesses granted and 171 accesses denied transactions for both PIV cards and temporary badges, we determined that we could not identify the person associated with the badge in any of the access granted transactions or the access denied transactions, unless the person's name was in the description field.

However, the IRS was able to identify 10 of the 40 temporary badges that were granted access for the ECC-Martinsburg using the two-step process previously mentioned. Those 10 transactions were for Calendar Year 2015 and had a unique number in the description field that was cross-referenced to information in the ePACS Enrollment Manager for the temporary badge including the badge number. However, this unique number was not present on the 10 transactions in the ECC-Martinsburg for 2014. Therefore, it appears that the ECC-Martinsburg was inputting a unique identifier for 2015 temporary badges in the description field. In most instances, the description field only included the type of temporary badge and not the badge number or unique identifier for the ECC-Martinsburg and the ECC-Memphis.

Without having the actual badge number in the transaction report, it is very difficult to determine the person who was issued the temporary badge, especially when a monthly reconciliation needs to be performed to determine who has accessed the computer rooms and tape libraries. Therefore, to enhance the current process of identifying badge numbers in transaction reports for easier verification on monthly reconciliations and other needs, such as incident research, AWSS organization officials have concluded that they can enhance the ePACS by creating a field for the unique badge identifier. We fully support this change to enhance the ePACS and make it easier to identify individuals gaining access with temporary badges.

Restricted Area Registers should be more detailed

The *Restricted Area Register* is currently used for documenting visitor information or contractor information for those who need a particular temporary badge to gain access to the computer rooms and tape libraries.

The IRM states that the *Restricted Area Register* will be maintained at the main entrance to the restricted area, and all visitors will be directed to the main entrance. Each person entering the restricted area, who is not assigned to the area, will sign the register. The restricted area monitor

[10] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

(staff) will complete the register by adding the individual's name, assigned work area, person to be contacted, purpose for entry, identification card number, and time and date of entry. The monitor will identify each visitor by comparing the name and signature entered in the register with the name and signature on some type of photo identification card, *i.e.*, government identification, driver's license. Upon verification of identity, the visitor will be issued an appropriate restricted area non-photo identification card. If the visitor is an IRS employee not assigned to the area, an exchange of identification cards will be made. Entry must be approved by the supervisor responsible for the area. Prior to exiting the area, the visitor will return the non-photo identification card to the monitor, and the monitor will enter the departure time in the register.

During our walkthroughs, we confirmed that the guard on duty will manually fill out the form and will require the person who is issued the temporary badge to sign for it. This form represents the official record for someone gaining access to the restricted area with a temporary badge.

We reviewed *Restricted Area Registers* for both the ECC-Memphis and the ECC-Martinsburg for Calendar Years 2014 through 2015, and identified some inconsistencies. Specifically,

- The ECC-Memphis has a more detailed register for obtaining the person's area of visitation within the restricted space; however, it did not capture the person's employment status. We could not determine whether the person was a contractor working for a vendor or an employee. Also, the information captured in the purpose section was either filled out with the word "work" or "cleaning," which we do not believe is descriptive enough.
- The ECC-Martinsburg did not capture a contact person's name if applicable for an escort. The guards only captured the person's last name in the print column, which does not help if there is another person with the same last name. The register did not capture the area or room in which the person was working or their purpose for being in the restricted area.

During our review, the IRS had standardized the *Restricted Area Register* by renaming it to the *Limited Area Register* and ensuring that the Organization column was present as well as the Work Area column. However, the person to be contacted and purpose for entry are not present on the updated form, and therefore does not comply with IRM requirements.

Although some information is captured for visitors or Level 2 access into the computer rooms and tape libraries, it is still difficult to identify the person if an incident were to occur because not enough information is captured by the registers. TIGTA believes that visitor information should be automated. For instance, by automating the visitor registration process, management will have reasonable assurance as to the identity of the individuals entering the restricted areas. Currently, registers are illegible and minimal information is recorded. Security could be improved if management entered visitor information into the ePACS. This would create an automated record with consistent essential information to identify the person who is associated

with the temporary badge. This would also provide more detailed information when the badge is used to actually identify who entered the computer room or tape library on a transaction report.

AWSS Physical Security office should maintain original Restricted Area Registers

Another observation was that the AWSS organization's Physical Security office personnel did not keep the original *Restricted Area Registers* when others requested them. For example, EOps organization personnel request the registers each month to perform reconciliations. The AWSS organization's Physical Security office personnel at the ECC-Martinsburg were sending the originals instead of sending copies to the other parties. As a result, we identified the following registers that were missing from the last two years:

- May 19-31, 2014, for the Annex.
- June 1-30, 2014, for the Annex.
- May 28-31, 2014, for the Main Building.
- July 1-7, 2014, for the Main Building.
- August 1-15 and 19-31, 2015, for the Main Building.

If an incident was to occur by a person with a temporary badge and the *Restricted Area Register* was missing, it would be very difficult to identify the person responsible for the incident. While on-site, we informed the AWSS organization's Physical Security office personnel that they need to keep the originals because these registers are their proprietary information. The IRM does not distinguish whether to keep the originals or copies. It only states that the registers are to be retained in a locked cabinet for two years. After we informed management of our concerns, they immediately changed their local procedures and now will keep the originals for two years as required by the IRM.

Enhancing the *Restricted Area Registers* to capture complete information regarding the official entry of the visitor, enhancing the ePACS to ensure a one-to-one match with the *Restricted Area Register* information, and using the PIV cards when appropriate will improve the security of the IRS. These improvements would allow the IRS to identify those individuals entering into the restricted computer rooms and tape libraries that house the IRS's critical infrastructure.

Recommendations

The Chief Information Officer, in coordination with the Chief, AWSS, should:

Recommendation 5: Align IRS policy and procedures with the HSPD-12 and Office of Management and Budget Memorandum M-05-24 by ensuring that employees and contractors working for more than six months are issued a PIV card with the appropriate access including limited area access, which can be authenticated by the ePACS.

Management's Response: The IRS disagreed with this recommendation, stating that it should not issue PIV cards based on length of time employees and contractors are with the IRS. The IRS believes that it is compliant with HSPD-12 and Office of Management and Budget M-05-24 guidelines regarding the issuance of PIV cards to employees and contractors. The IRS issues PIV cards to contractors who require routine (daily) unescorted access in accordance with Office of Management and Budget M-05-24.

Office of Audit Comment: Because the IRS does not issue PIV cards to all employees and contractors who need access to the restricted areas and have been employed for more than six months, we believe that the IRS is not fully compliant with Federal guidelines. We maintain that the IRS needs to align its policy and procedures with HSPD-12 and Office of Management and Budget M-05-24 guidelines to ensure that employees and contractors working for more than six months are issued PIV cards with the appropriate access including Limited access, especially because the IRS houses critical infrastructure and sensitive data within these restricted areas.

Recommendation 6: Configure the ePACS so temporary badge numbers or unique identifiers are visible in ePACS transaction reports.

Management's Response: The IRS agreed with this recommendation, stating that it implemented naming convention standards that provide visible temporary badge numbers and unique identifiers on the ePACS transaction reports.

Recommendation 7: Ensure that the *Limited Area Registers* are consistent and contain pertinent information that complies with IRS policy until an automated process is established.

Management's Response: The IRS agreed with this recommendation, stating that on August 17, 2016, the Chief, AWSS, issued an update to IRM 10.2.14, *Methods of Providing Protection*, requiring that Form 5421, *Limited Area Register*, must be used to document visitors to restricted areas.

Recommendation 8: Update policy to clarify that original *Limited Area Registers* be maintained within the Physical Security office and that copies can be disseminated to appropriate parties.

Management's Response: The IRS agreed with this recommendation, stating that in April 2016, the Physical Security office began providing an electronic report to the IT organization on a monthly basis. On August 17, 2016, the Chief, AWSS, issued an update to IRM 10.2.14, *Methods of Providing Protection*, stating that original *Limited Area Registers* must be maintained within the Physical Security office. The IRS is in the process of updating the IT organization's Standard Operating Procedures (SOP) to address dissemination.

Automating and Updating Access Monitoring Will Improve Security

Since 2014, the EOps organization has required the use of the Computer Room Access Form to authorize, recertify, and remove physical access to both the computer rooms and tape libraries. This form is a Portable Document Format (PDF) document which is digitally signed by the employee or contractor and submitted to their first-line manager for approval. It is then e-mailed to the EOps organization for second-level approval. Currently, the EOps organization, Chief ECC Project Response Incident and Management Office (PRIMO), or one of the designated staff, is responsible for authorizing access for both the computer rooms and tape libraries.

Required procedures were not always followed for authorization

According to EOps organization guidelines, each year, the EOps organization makes a data call via e-mail to individuals who have Level 1 and Level 2 access authorizations and requests that they recertify their access. An employee who needs access or continues to need access should request or recertify the authorization using the Computer Room Access Form and have it approved by his or her first-line manager. If the EOps organization does not receive a response from the data call, it is required to remove the individual's access to the computer rooms and tape libraries.

Prior to the Chief, ECC PRIMO, position taking over responsibility for overseeing the approval process in August 2015, the annual recertifications for authorizing access to the computer rooms and tape libraries for Fiscal Year 2015 at the ECC-Martinsburg location were not performed. However, the ECC-Memphis did perform the annual recertification for Fiscal Year 2015.

During the period December 2015 through March 2016, our analysis of the recertification log indicates the Chief, ECC PRIMO, was accepting and waiting on recertifications well past the required response date. TIGTA determined that, because this is a Facility Security Level 5 area, these individuals should have had their access immediately removed by the EOps organization after not responding to the initial data call requesting recertification. However, EOps organization management stated that the reason for the delay in recertifying these individuals was because they are addressing the Government Accountability Office recommendations[11] to ensure that only those employees who have a frequent and continuing business need to access a sensitive area are permitted to do so. The new approving official is working to educate the requestors and their managers and complete a one-for-one thorough review during the annual recertification process in hopes of using it to identify any additional gaps and educate everyone on the requirements.

[11] Government Accountability Office, GAO-14-405, *Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk* (Apr. 2014) and Government Accountability Office, GAO-15-337, *Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data* (Mar. 2015).

The IRS increased the risk of unauthorized individuals obtaining access to the computer rooms and tape libraries by reducing assurance that its critical infrastructure was adequately protected. Although there needs to be a continuity of operations, first-line managers should have responded timely to the data call. An automated process for notifying managers of the annual recertification would enhance controls for timely recertifications.

The EOps organization is not notified timely of access removal

Removal of access to computer rooms and tape libraries by the AWSS organization's Physical Security office is done when they are informed of access changes in one of three ways:

- A separated from IRS action has been submitted and the person appears in the Separating Employee Clearance system to initiate automated separating employee clearance modules, which automatically notifies Physical Security office personnel of a separation and that a manager has recovered an identification card.
- A manager informs his or her office that access is no longer needed.
- When notified by the EOps organization, Chief, ECC PRIMO, that access is no longer needed.

However, the Chief, ECC PRIMO, is not always notified when access is no longer needed. The EOps organization SOPs state that the first-line manager is supposed to notify the Chief by submitting the Computer Room Access Form through e-mail when an individual no longer needs access.

The Chief, ECC PRIMO, created a Removal Log in late Fiscal Year 2015 to assist in tracking the removal of employees who no longer needed access to computer rooms and tape libraries. When someone leaves the IRS or no longer needs access, the log is updated and the reason for removal is recorded.

TIGTA identified two instances using the Treasury Integrated Management Information System[12] separation database in which employees who were listed as no longer employed were not captured in the Removal Log. The cause for these instances was a breakdown in communication, which will sometimes prevent timely notification for removal of access. The first-line manager did not timely inform the Chief, ECC PRIMO, about the employees' separation and instruct that their access to the computer room and/or tape library be removed, and communication was lost when staff was transitioning in the Physical Security office. However, access was removed timely despite the lapse of communication.

Currently, when an employee is removed from access, the information goes into a database which Physical Security office personnel manually reconcile monthly to ensure that the

[12] Treasury Integrated Management Information System is an official automated personnel and payroll system for storing and tracking all employee personnel and payroll data.

employee is removed. In the event the first-line manager does not inform the Chief, the manual monthly reconciliation process should capture the removal because the AWSS organization's Physical Security office personnel should notify the Chief that they removed the person. Automating the removal process through an automated and secure system similar to the Online 5081 system would enhance the security of the access controls by bringing accountability to the process and limiting the potential for human error.

The manual authorization process is not effective or secure

We determined using the PDF forms as a means of approving access is not an effective or secure method of authorizing access to the restricted computer rooms and tape libraries. We reviewed 171 (70 percent) out of 246 Calendar Year 2014 PDF documents and determined two of the authorization forms were originally signed by first-line managers back in November 2011 and January 2013, and were resubmitted for authorization in Calendar Year 2014. We also identified two instances in which employees gained access by digitally signing for their first-line manager.

Our review of ePACS data from January 2014 through January 2016 identified 552 individuals (244 from the ECC-Memphis and 308 from the ECC-Martinsburg) who accessed the computer rooms or tape libraries. We found that 204 (37 percent) of the 552 individuals did not have an approved PDF Computer Room Access Form authorization on file. Figure 3 shows the number of employees by location.

Figure 3: Unauthorized Access by Individuals

Location	Individuals Who Did Not Have an Approved Access Form
ECC-Martinsburg	116
ECC-Memphis	88

Source: TIGTA analysis of the IRS's annual recertification data.

The Chief, ECC PRIMO, took over the position in late Fiscal Year 2015, and therefore could not account for all of the individuals identified in our analysis who accessed the computer rooms and tape libraries. As a result of our analysis, we requested that EOps organization management immediately remove the access of the employees who do not have an authorization on file and business need to enter the computer rooms and tape libraries.

Manually tracking more than 500 PDF documents is not an effective or efficient method of approving computer room and tape library access. It provides an environment for potential unauthorized access and an overall security risk to sensitive taxpayer information being compromised. These PDF forms are used to approve and allow access to the IRS's critical infrastructure which houses the most significant operations. Therefore, creating an automated process for approving and tracking access authorizations should provide management with the

necessary assurances to secure, prevent, and identify unauthorized access as well as increase efficiency.

Monthly reconciliations should include ePACS transactions

The Department of the Treasury requires[13] its bureaus to review physical access logs at least every 90 days, if not otherwise defined in formal bureau policy, and upon occurrence of bureau-defined events or potential indications of events.

On a monthly basis, the AWSS organization's Physical Security office runs an ePACS report showing the current list of names that are assigned access to the computer room and tape library door groups and sends the list to the EOps organization, Chief, ECC PRIMO. The Chief performs a manual monthly reconciliation of Level 1 computer room/tape library access. The reconciliation consists of the authorized list of names that the Chief retains and a comparison of the names from the ePACS report. This monthly reconciliation consists of comparing only authorized Level 1 names. Currently, Level 2 reconciliations consist of comparing the *Restricted Area Registers* against the Chief's records for those individuals who requested temporary or infrequent access.

Current EOps organization procedures for Level 1 access require the IT organization approving official (EOps organization, Chief, ECC PRIMO) to compare the names from the Level 1 Access List and validate their continued need for the level of access they have been granted, and delete from the approved access list individuals who no longer have a continued need to be in the computer room. An e-mail will then be sent by the EOps organization to the local AWSS organization's Physical Security office requesting the employees' access to the computer room be removed.

Using these procedures, the EOps organization is comparing names for only Level 1 employees and not reviewing who actually accessed the computer rooms, or how often they accessed them. Another ePACS report from the AWSS organization's Physical Security office can be obtained showing the actual access granted transactions for those who entered the computer rooms and tape libraries. By using this report, it can be determined who actually entered the computer rooms and tape libraries, so that unauthorized individuals can be identified. Currently, EOps organization procedures do not require a monthly review of the ePACS transaction reports. Without reviewing the actual entries into the computer rooms and tape libraries, the IRS is unaware if unauthorized individuals gained access.

Tape library management needs to be notified of access approvals

It is the responsibility of the local ECC Media Management Unit Chief with oversight of the tape library daily operations to obtain the appropriate access privilege of visitors to the restricted tape

[13] U.S. Department of the Treasury, TD P 85-01, Volume II, *Treasury Information Technology Security Program*, (June 2009).

library areas through the AWSS organization's Physical Security office and ensure that each visitor is physically escorted.

Currently at both the ECC-Martinsburg and the ECC-Memphis locations, the Chief, ECC PRIMO, grants second-level approval for access to the tape libraries and performs monthly reviews to reconcile access approvals. ECC Media Management, however, only approves access as the first-line manager, and therefore is unaware of Chief, ECC PRIMO, approval of contractors or visitors accessing the libraries. For example, cleaning contractors' authorizations go through the Contracting Officer Representative and the Chief, ECC PRIMO, and are never viewed or approved by the ECC Media Management. During our review, we did observe ECC Media Management personnel asking the AWSS organization's Physical Security office personnel to provide them with a monthly list of those who have accessed the library, which reflects their concern of not being made aware of second-level access approvals by the Chief, ECC PRIMO, to the tape library.

Although access to the tape library is approved by the EOps organization, it is from someone that is outside of ECC Media Management. We determined that coordination and oversight is needed between the Chief, ECC PRIMO, and ECC Media Management to ensure that both parties are notified of who has approval access to tape libraries. Without local staff knowledge of the people entering and exiting the tape library, security may be easily compromised as the tape library houses highly sensitive transportable magnetic media.

Frequency access controls are not working

When the new Chief, ECC PRIMO, took over the access monitoring, he or she changed the controls for the Level 1 and Level 2 access. The new World Class Data Center Vision is not to have anyone continuously in the computer rooms. Therefore, a permanent presence in the computer room is no longer applicable. Although the Computer Room Access Form was changed to show that Level 1 access is now based on permanent badge access, such as teleworking system administrators, and Level 2 is occasional, intermittent access, we determined that the EOps organization SOPs need to be updated so that frequency is not a factor. The SOPs still show Level 1 access being a continuing and frequent need to access the computer room and Level 2 is intended for individuals who require computer room access on an occasional basis.

Prior to the new Chief, ECC PRIMO, taking over, we determined that the Level 1 and Level 2 controls based on frequency established by the EOps organization were not being followed. The previous SOPs established frequent access for Level 1 as more than 15 times per month based on the EOps organization SOPs Exhibit B. Level 2 access is intended for individuals who require computer room access on an occasional basis (fewer than 15 times per month). Currently, the Chief, ECC PRIMO, is not monitoring the access into the computer room through ePACS transactions. He or she is mainly relying on the manager's word on how often access is needed. The Chief also stated that he or she is performing spot checks on the frequency; however, we did not see evidence of this check. We reviewed the frequency of access for both the ECC-Martinsburg and the ECC-Memphis from ePACS data for Calendar Year 2015.

Figure 4 shows the total number of employees who accessed the computer rooms and tape libraries fewer than the required number of times necessary to retain the Level 1 status.

Figure 4: Analysis of Number of Accesses by Level 1 Employees

Location	Computer Rooms Accessed by Level 1 Users Fewer Than 15 Times per Month
ECC-Martinsburg	158 out of 239 people
ECC-Memphis	140 out of 173 people

Location	Tape Libraries Accessed by Level 1 Users Fewer Than 15 Times per Month
ECC-Martinsburg	88 out of 108 people
ECC-Memphis	43 out of 46 people

Source: TIGTA analysis of IRS Calendar Year 2015 ePACS data.

For Level 2 access, the person checks in at the guard station to receive a temporary badge which allows them access into the computer rooms. We reviewed a judgmental sample[14] from the handwritten *Restricted Area Registers* for the months of January and July 2014 and January and July 2015, for seven maintenance contractors at the ECC-Martinsburg location and seven cleaning contractors at the ECC-Memphis location. Figure 5 shows the number of contractors who accessed the computer rooms more than the required number of times necessary to retain the Level 2 status.

Figure 5: Analysis of Number of Accesses by Level 2 Contractors

Location	Level 2 Contractors Who Accessed the Computer Room More Than 15 Times per Month
ECC-Martinsburg	5 of 7 contractors
ECC-Memphis	5 of 7 contractors

Source: TIGTA analysis of IRS Restricted Area Register data.

We also determined that the ePACS cannot distinguish between a Level 1 and Level 2 user. If a person has an HSPD-12 PIV, the system will record the person's name associated with the credential. Although the majority of the names in the ePACS are associated with a Level 1 user, we could not distinguish the level without reviewing the authorization. This creates confusion during the monthly reviews because the AWSS organization's Physical Security office has the

[14] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

ability to send the EOps organization only a list of names that have access to the computer rooms and cannot distinguish between Level 1 and Level 2.

We support the EOps organization's decision to change the access control and suggest that it defines the permanent badge access, or Level 1, as those with a business need who are employed for more than six months, which follows the HSPD-12 guideline. Those employed fewer than six months with an official business need would receive a Level 2 access.

Computer room and tape library access is only for official business needs

We reviewed procedures for emergency situations, such as an event that would be detrimental to the operations of the computer rooms, and determined that the AWSS organization's Physical Security office escorts those with an official need to help with emergencies. Authorization is approved for these individuals.

However, we identified an instance in which the family of an authorized Level 1 employee was approved to tour the computer room. We could not determine which family members actually accessed the computer room because the *Restricted Area Registers* were missing for that day. The EOps organization approved the family members' access to the computer room based on IRM 11.3.1.13, dated March 7, 2008, that states:

- Relatives of IRS employees have no right to access or receive confidential information based on their relationship to the IRS employee. Potential criminal and civil penalties under Internal Revenue Code Sections (§§) 7213, 7213A, and 7431; 5 U.S.C. § 552; and 18 U.S.C. § 1905, among others, could apply to such accesses/disclosures.
- When IRS employees bring relatives, *e.g.*, children, into their work environment, care must be exercised to ensure that the visitors are not exposed to confidential information verbally, on computer screens, or in hard copy. It does not matter whether the visitors have an interest in the material or understand the technical work-related meaning of the information. During "Take Your Children to Work Day," children cannot have access to confidential information while parents explain their job or tour the work environment, *etc*. Even simple tasks such as photocopying could involve inappropriate access to confidential information. Exposure to confidential information is not allowed and can have severe consequences.
- Relatives must not accompany employees during field compliance activities in which the accompaniment itself could reveal who has a tax liability, who is being examined, *etc*.

However, TIGTA identified IRM 10.2.14.5, that was more current, dated September 23, 2009, for restricted areas. It states:

- A Restricted Area is an area to which access is limited to authorized personnel only. Restricted area space can be identified by Physical Security and Emergency Preparedness

Territory managers based on critical assets. All restricted areas must meet secured area requirements.

- Restricted areas shall have signs prominently posted as a "Restricted Area" and be separated from other areas by physical barriers which will control access. The number of entrances will be kept to a minimum and each entrance controlled. Adequate control will be provided by locating the desk of a responsible employee at the entrance to assure that only authorized persons, **with an official need**, enter. Only individuals assigned to the area will be provided Restricted Area identification cards.

We also identified the ECC-Martinsburg Facility Access Memorandum, dated February 7, 2014, that states:

- Any visitor to ECC-Martinsburg (including IRS, Federal, or contract employee with a verified completed background investigation) who has a work-related need to go into the computer room, tape library, or other restricted space must receive approval of the senior Mainframe Operations Branch official on duty. **Access to restricted areas is limited to those with a verified business need.** Once approval is given, they must sign in on the Restricted Access Register in the building lobby and will require an escort while in the restricted space.

When computer room access is granted without an official business need, it is a significant security risk to allow accessibility to mainframes and other technology equipment and systems. It risks the safety of the equipment and the data residing on that equipment. These systems are essential to the overall operation of the IRS.

Recommendations

The Chief Information Officer should:

Recommendation 9: Update current policy to require the use of a secure automated system to authorize and remove physical access to the computer rooms and tape libraries.

Management's Response: The IRS disagreed with this recommendation, stating that the manual process in place works and adequately mitigates any risks. While automation is a preferable option, it is not a requirement to meet the standards, and funds spent on automation must be weighed against other priorities.

Office of Audit Comment: The current manual process to authorize individuals entering the Facility Security Level 5 computing centers is not effective, timely, or secure, as identified during our audit. We maintain that automation will enhance the physical access controls by ensuring that the authorization process of individuals is securely and timely approved by the appropriate manager, and access is removed timely if the annual authorization is not completed.

Recommendation 10: Update policy and forms to provide oversight to ensure that the Chief, ECC PRIMO, coordinates with tape library management on the approvals to tape library access.

> ***Management's Response:*** The IRS agreed with this recommendation, stating that it updated the policy on April 25, 2016, and is updating the IT organization's SOPs to require this change.

Recommendation 11: Update procedures for the monthly reconciliation of computer room and tape library ePACS access logs as required by Department of the Treasury guidance. The ePACS report should show the actual accesses during the month to identify all persons who entered the computer rooms and tape libraries, and to determine if all the persons were authorized with an official business need to enter.

> ***Management's Response:*** The IRS partially agreed with this recommendation, stating that it will clarify the definition of business need as part of the policy guidance. The IRS disagreed that the procedures for monthly reconciliation of computer room and tape library access logs should be updated to show the number of times someone entered those rooms. Access is granted based on official business need, not frequency of access. Review of how many times a person accesses the room is not a requirement.
>
> ***Office of Audit Comment:*** During our audit, we found that the IRS did not specifically know who enters the computer rooms or tape libraries because it only reviews who is authorized to be in those rooms and not who actually accessed those rooms in the access report. We maintain that, to facilitate the monthly reconciliation process, the ePACS report should include the actual accesses that occurred during the month to identify all persons who entered the computer room and tape library, and compare those access to those authorized for access.

Recommendation 12: Update policy to change or remove the Level 1 and Level 2 designations based on frequency of access, and use access designations that align with the HSPD-12 guidelines and reflect the level of business need.

> ***Management's Response:*** The IRS disagreed with this recommendation, stating that the Level 1 and Level 2 designations for access to the computer room for a given period of time are based on business need rather than how many times someone accesses an area.
>
> ***Office of Audit Comment:*** The latest SOPs are still based on frequency of access and still show Level 1 access being a continuing and frequent need to access the computer room and Level 2 is intended for individuals who require computer room access on an occasional basis.

Recommendation 13: Clarify and update all IRS policy to require that restricted area access must have a verified official business need.

Management's Response: The IRS disagreed with this recommendation, stating that current IRS policy requires that restricted area access must have an official business need. As referenced in its response to Recommendation 11, the IRS is updating IRS policy to clarify the definition of official business need.

Office of Audit Comment: We maintain that all IRS policy needs to be clarified and updated to require that restricted area access must have a verified official business need.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the controls in place to restrict access to computer rooms and tape libraries, and to prevent and detect unauthorized accesses to those resources. To accomplish our objective, we:

I. Determined if Level 1[1] controls for frequent access to computer rooms and tape libraries sufficiently detect, deter, and prevent unauthorized access.

A. Determined computer room access policy for each location and if policy is consistent for different locations.

B. Determined if unauthorized access existed at the computer rooms and tape libraries by obtaining and reviewing ePACS data from January 2014 through January 2016. We determined that the data were reliable because we performed additional ePACS readers and door group testing prior to the download, and we used a third party to verify that all data transactions were successfully transferred from the IRS to TIGTA. Our frequency test included the entire population for Calendar Year 2015 from our download. Our scope did not include identifying the appropriate background investigations for Level 1 users due to time constraints.

C. Determined if removal procedures for Level 1 access are working.

II. Determined if the Level 2 controls for occasional access to the computer rooms and tape libraries sufficiently detect, deter, and prevent unauthorized access.

A. Determined if computer room and tape library access policy is consistent and sufficient for different locations.

B. Determined if unauthorized access existed at the computer rooms and tape libraries by obtaining ePACS data from January 2014 through January 2016. We determined that the data were reliable because we performed additional ePACS readers and door group testing prior to the download, and we used a third party to verify that all data transactions were successfully transferred from the IRS to TIGTA. Level 2 tests in Figures 2 and 5 used judgmental samples[2] because these transactions had to be matched back to the manual records. Our scope did not include identifying the appropriate background investigations for Level 2 users due to time constraints.

C. Determined if removal procedures for Level 2 access are working.

[1] See Appendix IV for a glossary of terms.
[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

III. Determined if any other parties (outside of Level 1 and 2) are entering computer rooms or tape libraries and how they obtained access.

A. Determined if emergency procedures are warranted and sufficient.

B. Determined if any other reasons for obtaining computer room or tape library access were warranted in the last two years and who authorized it. (This was identified by manually reviewing log books and who requested a temporary identification badge who may not have been in the computerized system.)

IV. Determined the current state of security for computer rooms and tape libraries and whether upgrades are in progress.

A. Determined if periodic security camera reviews are performed for the computer rooms and tape libraries to monitor for unusual or questionable activities.

B. Determined the current Facility Security Level of the computer rooms and tape libraries at each of the locations.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*;[3] Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive 12—Policy for a Common Identification Standard for Federal Employees and Contractors*;[4] FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;[5] Draft NIST Special Publication 800-116 Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*;[6] and related IRS guidelines for gaining, monitoring, and removing access to computer rooms and tape libraries. We evaluated these controls by conducting interviews and meetings with the IT organization's EOps and AWSS organizations. We also reviewed the IRS's surveillance controls for the computer rooms and tape libraries.

[3] U.S. Department of Homeland Security, Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, (Aug. 2004).
[4] Office of Management and Budget, M-05-24, *Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 2005).
[5] U.S. Department of Commerce, Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*, (Aug. 2013).
[6] U.S. Department of Commerce, NIST Special Publication 800-116, Revision 1, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* (Dec. 2015).

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph F. Cooney, Audit Manager
Cari Fogle, Lead Auditor
Naomi Butler, Senior Auditor
George L. Franklin, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Chief, Agency-Wide Shared Services
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User Network Services
Chief, Enterprise Computing Center - Project Response Incident and Management Office
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Access Controls	A policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: i) passing the information to unauthorized subjects or objects; ii) granting its privileges to other subjects; iii) changing one or more security attributes on subjects, objects, the information system, or system components; iv) choosing the security attributes to be associated with newly created or modified objects; or v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges, *i.e.*, they are trusted subjects, such that they are not limited by some or all of the above constraints.
Agency-Wide Shared Services	Its mission is to provide complete, professional, Equal Employment Opportunity and Diversity Field Services (Treasury Complaint Mega Center), Employee Support Services, Real Estate and Facilities Management, and Physical Security and Emergency Preparedness services to all organizational entities within the IRS.
Card Reader	Located at access points for controlled resources where a cardholder may wish to gain access (physical and logical) by using the PIV card. The reader communicates with the PIV card to retrieve the appropriate information located in the card's memory to relay it to the access control systems for granting or denying access.
Contracting Officer Representative	The Contracting Officer's Representative is the principal program representative assigned to Government procurements. The primary role of the Contracting Officer's Representative is to provide technical direction, monitor contract performance, and maintain an arm's-length relationship with the contractor, ensuring that the Government pays only for the services, materials, and travel authorized and delivered under the contract.

Term	Definition
Controlled Area	Any area or space for which an organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Critical Infrastructure	Physical and cyber systems and assets so vital to the United States that their incapacity or destruction would have debilitating effects.
Enrollment Manager	Enrollment Manager is a Velocity database tool for enrolling users and flexibly associating data with users' credentials. Enrollment Manager enables very detailed information collection per user. It is used to organize information for a given user. When enrolling someone in the system, be sure to provide some kind of unique identifier, *e.g.*, Standard Employee Identifier. Devices such as scanners can be installed to capture data from business cards or PIVs to reduce the need for manual data entry.
Enterprise Operations	An IRS IT organization responsible for providing efficient, cost effective and highly reliable computing (server and mainframe) services for all IRS business entities and taxpayers.
Enterprise Physical Access Control System	A system for controlling access to facilities seeking Federal Government compliance with HSPD-12 by implementing Public Key Infrastructure (encryption) in the ePACS. The System operates with all modern credentials.
Facility Security Level 5	Each Federal facility has unique attributes that reflect its individual security needs and the missions of the Federal tenants. Level IV—buildings with 150,000 square feet or more, more than 450 Federal employees, and a high level of public access; and Level V—buildings that are similar to Level IV but are considered critical to national security, *e.g.*, the Pentagon.
Federal Information Processing Standard 201	A U.S. Federal Government standard that specifies PIV requirements for Federal employees and contractors.

Term	Definition
Homeland Security Presidential Directive - 12	Directive which mandates a Federal standard to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Governmentwide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Level 1 Access	Access granted to individuals who maintain a permanent presence in the computer room or require daily entry into the computer room to perform their duties as determined by the approving official.
Level 2 Access	Access granted to individuals who have a business need to enter the computer room on an occasional basis.
Master File	A computer record containing information about taxpayers' filing of returns and related documents for both individual tax returns, *i.e.*, Individual Master File, and business tax returns, *i.e.*, Business Master File. The Master File contains information on the current year plus all years that have had activity within the two previous years. In addition, the Master File maintains retention register files on taxpayers for two additional years. (Note: Older tax return data with less information than current year cases are maintained on microfilm for an indefinite period of time.)
National Institute of Standards and Technology	Under the Department of Commerce, this organization is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Online 5081 System	A web-based application and is currently the system used to obtain access to needed systems.

Term	Definition
Personal Identification Number	A short numeric password (six to eight digits) used as an authenticator by the PIV card to authenticate the cardholder.
Personal Identity Verification	A U.S. Federal smart card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assures appropriate levels of security for all applicable Federal applications.
Two-Factor Authentication	A method of confirming a user's claimed identity by using a combination of two different components. These components may be something that the user knows, something that the user possesses, or something that is inseparable from the user.
World Class Data Center Vision	Two physical data centers efficiently laid out to maximize efficiency and the Cloud; no operations employees in the computer room floor; operations employees on-call for installations and other hardware support, such as support to hardware contractors; and no caged area in the computer room. The data centers will provide information technology and facility infrastructure to house the IRS, Department of the Treasury, TIGTA, and other department/agency information technology infrastructure in a secure (Level 5) environment with a chargeback model for computing services (rent, utilities, network, bandwidth, *etc*.) established through a memorandum of agreement or service level agreement.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 15, 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL AUDIT

FROM: S. Gina Garza
Chief Information Officer

Kevin McIver
Chief, Agency-wide Shared Services

SUBJECT: Draft Audit Report- Security and Computing Center Access Privileges - #201620010

Thank you for the opportunity to review the draft audit report and provide comments on security and access privileges at IRS's computing centers. Security at our computing centers is a high priority for the IRS, and we make every effort to operate our centers in line with current federal policy to deter potential threats. We appreciate TIGTA's recognition of the critical nature of IRS systems and the data that resides in our computing centers, in particular on our mainframes, servers, and other technology equipment, as well as back-up tapes for operations.

We agree with a number of the recommendations in your draft report, and have implemented many of them as outlined in the attachment. However, we do have concerns that some of your recommendations do not take into account the current mandated standards, which we have discussed with your team on various occasions throughout the audit. An example of this is your recommendation to automate processes and procedures to authorize physical access to IRS computer rooms and tape libraries. This is an area where in fact our current processes are meeting mandated standards and have been quite effective. While we truly appreciate the value of exceeding standards with more automation in this area, it does not rise to the level of other more pressing priorities.

In closing we want to thank your team for identifying areas where we need to improve security at our computing centers. The IRS values the analysis and recommendations associated with our access controls and business processes. If you have any questions, please contact Gina Garza at (202) 317-5000, Kevin McIver at (703) 414-2143, or Karen Mayr on (202) 368-8396.

Attachment

Attachment

RECOMMENDATION #1:

The Chief, Agency-Wide Shared Services should update the ePACS policy, specifically, the Physical Security Operations Guide and the ePACS Operation Manual, to require testing of the programming of impacted cards when a door group is established or modified, and annually to ensure that access is properly controlled to restricted or limited areas.

CORRECTIVE ACTION:

IRS agrees with this recommendation. The Chief, Agency-Wide Shared Services, will update the ePACS Installation Checklist to require annual testing of the programming of impacted cards when a door group is established or modified, to ensure that access is properly controlled to restricted or limited areas.

IMPLEMENTATION DATE:

February 15, 2017

RESPONSIBLE OFFICIAL:

Director, Facilities Management and Security Services, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:

IRS will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #2:

The Chief, Agency-Wide Shared Services should implement a FIPS 201 compliant two-factor authentication for the computer rooms and tape library at the ECC-Memphis.

CORRECTIVE ACTION:

IRS agrees with this recommendation. IRS plans to install readers that will require PIN authentication for computer rooms at the ECC-Memphis.

IMPLEMENTATION DATE:

July 30, 2017

RESPONSIBLE OFFICIAL:

Director, Facilities Management and Security Services, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:

IRS will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #3:

The Chief, Agency-Wide Shared Services should repair or update security surveillance equipment and ensure automatic security camera pan functions properly at the perimeters of Limited areas when an alarm is triggered.

CORRECTIVE ACTION:

IRS agrees with the need to repair the camera, and completed that repair in July 2016, but we do not agree with updating the camera software to include automated panning, as that is above the current standard.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION #4:

The Chief, Agency-Wide Shared Services should update and include details in procedures and guidelines for monitoring physical intrusion alarms and surveillance equipment, such as security camera monitoring and recording, automatic backup capabilities for the DVRs, and an alarm to alert security personnel when an active DVR has failed.

CORRECTIVE ACTION:

IRS disagrees with this recommendation. The IRS is compliant with the Interagency Security Committee's "Risk Management Process for Federal Facilities" dated January 7, 2016 that requires CCTV on limited access points. TIGTA's recommendation is above the standard required for federal facilities.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION #5:

The Chief Information Officer, in coordination with the Chief, Agency-Wide Shared Services should align IRS policy and procedures with HSPD-12 and Office of Management and Budget memorandum M-05-24, by ensuring that employees and contractors working for more than six months are issued a PIV card with the appropriate access including Limited area access, which can be authenticated by the ePACS.

CORRECTIVE ACTION:

The IRS disagrees with the recommendation that IRS should issue PIV cards for contractors based on length of time they are with IRS. The IRS is compliant with HSPD-12 and OMB M-05-24 guidelines regarding the issuance of PIV cards to employees and contractors. IRS issues PIV cards to contractors who require routine (daily) unescorted access in accordance with OMB M-05-24.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION # 6:

The Chief Information Officer, in coordination with the Chief, Agency-Wide Shared Services should configure the ePACS so temporary badge numbers or unique identifiers are visible in ePACS transaction reports.

CORRECTIVE ACTION:

IRS agrees with this recommendation. IRS implemented naming convention standards that provide visible temporary badge numbers and unique identifiers on the ePACS Velocity Personal Information transaction reports.

IMPLEMENTATION DATE:

Completed July 28, 2016

RESPONSIBLE OFFICIAL:

Director, Facilities Management and Security Services, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION #7:

The Chief Information Officer, in coordination with the Chief, Agency-Wide Shared Services should ensure that the Limited Area Registers are consistent and contain pertinent information that complies with IRS policy until an automated process is established.

CORRECTIVE ACTION:

IRS agrees with this recommendation. On August 17, 2016, the Chief, Agency-Wide Shared Services, issued an update to IRM 10.2.14, *Methods of Providing Protection*, requiring that Form 5421, *Limited Area Register*, must be used to document visitors to restricted areas.

IMPLEMENTATION DATE:

Completed August 17, 2016

RESPONSIBLE OFFICIAL:

Director, Facilities Management and Security Services, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION #8:

The Chief Information Officer, in coordination with the Chief, Agency-Wide Shared Services, should update policy to clarify that original Limited Area Registers be maintained within the Physical Security office and that copies can be disseminated to appropriate parties.

CORRECTIVE ACTION:

IRS agrees with this recommendation. In April 2016, the Physical Security Office began providing an electronic report to IT on a monthly basis. On August 17, 2016, the Chief, Agency-Wide Shared Services, issued an update to IRM 10.2.14, *Methods of Providing Protection,* stating that original Limited Area Registers must be maintained within the Physical Security office. IRS is in the process of updating the IT Standard Operating Procedure to address dissemination.

IMPLEMENTATION DATE:

January 15, 2017

RESPONSIBLE OFFICIAL:

ACIO, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN:

IRS will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #9:

The Chief Information Officer should update current policy to require the use of a secure automated system to authorize and remove physical access to the computer rooms and tape libraries.

CORRECTIVE ACTION:

IRS disagrees with this recommendation since the manual process in place works and adequately mitigates any risks. While automation is a preferable option, it is not a

requirement to meet the standards, and funds spent on automation must be weighed against other priorities.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION #10:

The Chief Information Officer should update policy and forms to provide oversight to ensure that the Chief ECC PRIMO coordinates with tape library management on the approvals to tape library access.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The IRS updated the policy April 25, 2016 and is updating the IT Standard Operating Procedure to require this change.

IMPLEMENTATION DATE:

January 15, 2017

RESPONSIBLE OFFICIAL:

ACIO, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN:

IRS will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #11*:*

The Chief Information Officer should update procedures for the monthly reconciliation of computer room and tape library e-PACS access logs as required by Treasury guidance. The ePACS report should show the actual accesses during the month to

identify all persons that entered the computer rooms and tape libraries and to determine if all the persons were authorized with an official business need to enter.

CORRECTIVE ACTION:

IRS partially agrees with this recommendation. The IRS disagrees with the portion of the recommendation that the procedures for monthly reconciliation of computer room and tape library access logs should be updated to show the number of times someone entered those rooms. Access is granted based on official business need, not frequency of access. Review of how many times a person accesses the room is not a requirement. However, IRS will clarify the definition of business need as part of the policy guidance.

IMPLEMENTATION DATE:

December 15, 2016

RESPONSIBLE OFFICIAL:

ACIO, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN:

IRS will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #12:

The Chief Information Officer should update policy to change or remove the Level 1 and Level 2 designations based on frequency of access and use access designations that align with the HSPD-12 guidelines and reflect the level of business need.

CORRECTIVE ACTION:

The IRS disagrees with this recommendation. The Level 1 and Level 2 designations for access to the computer room for a given period of time are based on business need rather than how many times someone accesses an area.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

RECOMMENDATION #13:

The Chief Information Officer should clarify and update all IRS policy to require that restricted area access must have a verified official business need.

CORRECTIVE ACTION:

The IRS disagrees with the need for this recommendation. Current IRS policy requires that restricted area access must have an official business need. As referenced in our response to Recommendation #11, IRS is updating IRS policy to clarify the definition of official business need.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A