WHITE OAK
SECURITY

Federal Reserve Bank of Minneapolis

Minimum Wage System Controls Review

May 18, 2021

Table of Contents

Scope Summary

Project	Minimum Wage System Controls Review
Report Version Number	1.3

Engagement Summary

Assessor	Brett DeWall
Test Date	April 15th, 2021
Goals	The engagement focused on assessing Federal Reserve Bank of Minneapolis's minimum wage computer system to identify gaps in the current control environment and ensure a full coverage of security requirements.
Limitations	None

Executive Summary

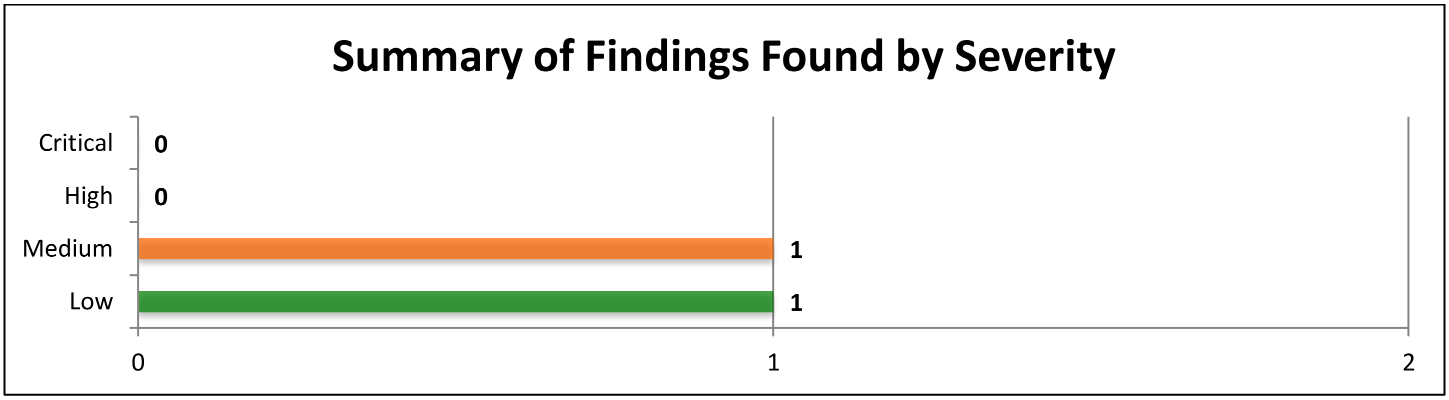
On April 15th, 2021 Federal Reserve Bank of Minneapolis (FRB MPLS) engaged White Oak Security to perform a Controls Review Assessment of their Minimum Wage System.

The engagement focused on assessing FRB MPLS's deployment of their Minimum Wage System along with meeting configuration controls laid out by the state of Minnesota. The goal of this testing was to validate each of the control details with comparison to FRB MPLS's Minimum Wage System setup.

During the course of the assessment White Oak Security discovered two (2) issues. The installed anti-malware software was utilizing an out-of-date definitions repository of over a year old. FRB MPLS implemented new changes as part of the quarterly update process to ensure the anti-malware definitions stay up-to-date. Another issue identified involved paper media discovered around the Minimum Wage System workspace. The paper media discovered did not contain classified data, however White Oak recommends that FRB MPLS instruct researchers to utilize existing lockable cabinets within the room to store any paper media.

White Oak Security rated the identified control failures in terms of Business Impact to the organization. The following is a summary of the control requirements along with the observation obtained while onsite.

During the engagement, White Oak Security identified two (2) findings including **zero (0) Critical-Risk** issues, **zero (0) High-Risk** issues, **one (1) Medium-Risk** issue, and **one (1) Low-Risk** issue.



Findings Table Ratings

The *Business Impact* rating estimates the severity of a potential attack based on information gathered during the security assessment.

Business Impact

Rating	Description	CVSS Score
Low	Little to no adverse impact, monetary or otherwise.	0.1 – 3.9
Medium	Limited and/or quantifiable financial impact; possible negative media exposure.	4.0 – 6.9
High	Significant financial impact; probable negative media exposure; damage to reputation capital.	7.0 – 8.9
Critical	Immediate significant financial impact; probable negative media exposure; damage to financial reputation capital	9.0 – 10.0

Detailed Review Details

The *Detailed Findings* table describes control names, control details, and the observation observed during the testing. Findings are arranged in order of control standards required for the workstation.

Enterprise Identity and Access Management Standard

Control Name	Control Detail	White Oak Observation
1. Access Control	All access to systems or data must be controlled through the use of identification and authentication mechanisms. This access control must: • Assign privileges to individuals based on the individual's job classification and function. • Restrict privileges to the least needed for the individual or service to perform their role. • Deny all access that is not explicitly granted. • Remove all system access not explicitly required.	White Oak reviewed user accounts and corresponding job functions and determined all accounts were appropriately provisioned based on job access requirements and least privilege. No control deficiencies noted.
2. Unique IDs	All users must be assigned a unique ID to access systems or data. IDs must not be reused for at least 10 years.	White Oak reviewed user accounts and determined all accounts were assigned unique IDs. No control deficiencies noted.
3. Device, Service, and Application Accounts	Device, service, and application accounts must be assigned to an account owner and must not be used by individuals to access the system.	White Oak reviewed all device, service, and application accounts to determine FRB MPLS meets this control requirement. No control deficiencies noted.
4. Access Approval	Requests to create or modify accounts and access privileges must be documented and approved by authorized personnel before access can be granted. Each request for access must define access needs including: • Systems and data that each user needs to access for their job function. • Level of privilege required (for example: user administrator, etc.) for accessing resources.	White Oak reviewed the access approval process and determined all requests meet the requirements for access. No control deficiencies noted.
5. Account Review	All accounts must be reviewed upon changes in user role and at least annually for user account and every 6 months for privileged accounts and service accounts. The review must validate and recertify that all access privileges are still needed and authorized. The results of the review must be documented and unnecessary access privileges must be communicated to account administrators for removal. Review documentation must be maintained by the account administrator for at least 2 years and made available to central access control team upon request.	White Oak reviewed the implemented process for account review and determined that FRB MPLS met the control objective. No control deficiencies noted.
6. Inactive Accounts	Inactive accounts must be disabled after no more than 90 days of inactivity. Disabled accounts must be deleted within 1 year.	White Oak reviewed user accounts to determine that no currently implemented accounts need to be disabled. Furthermore, there hasn't been an instance yet in which an account needed to be disabled. No control deficiencies noted.

7. Revoke Access	Accounts and privileges that are no longer required must be removed or disabled within: • 8 hours of notification or identification of voluntary changes in access. • 1 hour of notification or identification for users that have been involuntarily terminated or for accounts with credentials that may have been lost or compromised.	White Oak reviewed the implemented process and determined that FRB MPLS meets this control requirement. An account hasn't been revoked from this system yet to have a log of events. No control deficiencies noted.
8. Emergency Accounts	Emergency and temporary accounts must be disabled within 24 hours.	White Oak discovered no emergency accounts implemented on the system. No control deficiencies noted.
9. Privileged Accounts	Privileged IDs must be: • Approved by the system owner. • Assigned only to users that specifically require such privileged access. • Restricted to least privileges necessary to perform administrative responsibilities. • Granted access to only the system utilities that are needed. • Authenticated user uses multifactor authentication when accessing systems with data protection categorization of High. • Prohibited from changing privileges to another user ID either for themselves or another user without authorization.	White Oak reviewed the approval process and implemented user accounts. No control deficiencies noted.
10. Separate Administrative Account	Privileged IDs must only be used when performing authorized administrative tasks. Non-privileged accounts must be used when performing all other tasks.	White Oak reviewed implemented user accounts and determined that administrative tasks are performed utilizing only authorized accounts and non-privileged accounts are used for all other tasks. No control deficiencies noted.
11. Segregation of Duties	Access privileges must allow for the appropriate segregation of duties by: • Segregating duties of individuals as necessary, to prevent malicious activity without collusion. • Ensuring that audit functions are not performed by personnel responsible for administering access control. • Maintaining a limited group of administrators (i.e. system administrators, application administrators, security administrators) with access based upon the users' roles and responsibilities. • Ensure that critical functions and system support functions are divided among separate individuals. • Ensure that system testing functions and production functions are divided among separate individuals or groups.	White Oak reviewed and witnessed the segregation of duties utilized for accessing and maintaining the Minimum Wage System. No control deficiencies noted.

12. Vendor Access	Accounts used by vendors to access, support or maintain system components via remote access must be: • Enabled only during the time period needed. • Disabled when not in use. • Monitored when in use.	No vendor accounts have been created for the Minimum Wage System. No control deficiencies noted.
13. Group Accounts	Group, shared, or generic IDs password or authentication methods must be restricted as follows: • Generic user IDs must be disabled or removed. • Shared user IDs must not exist for system administration and other critical functions. • Shared and generic user IDs must not be used to administer any system components. • Passwords and other credentials for group / role accounts must be changed when someone leaves the group / role.	No group accounts have been created for the Minimum Wage System. FRB MPLS does make use of specific firecall checkout accounts that do follow all required controls. No control deficiencies noted.
14. Authentication	All users and administrators must be authenticated on all systems by using at least one of the following methods: • Something you know, such as password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as fingerprint.	White Oak determined all users utilize passwords to log into the Minimum Wage System. No control deficiencies noted.
15. User Validation	The user's identity must be properly validated before modifying or communicating any authentication credential – for example, performing password resets, provisioning new tokens or generating new keys.	FRB MPLS's procedures properly validate users before modifications or before any communication of credentials occurs. No control deficiencies noted.
16. First Time Passwords	First-time use and reset passwords / phrases must be: • Set to a unique value for each user. • Changed immediately after the first use.	The first-time password is set to a unique password and is required to be changed upon first login on the Minimum Wage System. No control deficiencies noted.
17. Password Encryption	All authentication credentials (such as passwords / phrases) must be encrypted during transmission and storage.	White Oak determined that all authentication credentials meet the encryption requirements. No control deficiencies noted.
18. Password Length	Passwords must be at least: • 8 characters long for user accounts and all mainframe accounts. • 12 characters long for privileged accounts. • 14 characters long for device, service, and application accounts.	White Oak determined that all user accounts require a minimum of 14-character passwords. No control deficiencies noted.

19. Password Complexity	Passwords must contain at least: • 3 of the 4-character types below for user accounts and all mainframe accounts. • 4 of the 4-character types below for privileged accounts and device, service, and application accounts. • Character Types: o Lower case letters. o Upper case letters. o Numbers. o Special characters.	White Oak determined that all user accounts require password complexity on all passwords. No control deficiencies noted.
20. Minimum Password Age	Passwords / passphrases must be in place for at least 1 day. Mainframe account passwords must be in place for at least 5 days.	White Oak determined that all user accounts require a minimum password age of 7 days. No control deficiencies noted.
21. Maximum Password Age	Passwords / passphrases must be changed at least: • Every 90 days for user accounts. • Every 60 days for privileged accounts. • Every 180 days for device, service, and application accounts. • Every 30 days for mainframe accounts.	White Oak determined that all user accounts require a maximum password age of 90 days. The Department of Revenue has provided written approval of this implementation. No control deficiencies noted.
22. Password History	New passwords / phrases must be different from at least the previous 24 passwords / phrases used by that account.	White Oak determined that all user accounts require a password history of 24 passwords. No control deficiencies noted.
23. Non-Password Authentication	Where authentication mechanisms other than passwords are used (for example, physical or logical security tokens, smart cards, certificates, etc.) these mechanisms must be controlled as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and / or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. • A defined registration process must be established for issuing, maintaining and retrieving hardware tokens. When issuing a hardware token, the individual receiving the token must be authorized and verified in person by a designated official.	White Oak determined that no non-password authentication mechanisms were in use with the Minimum Wage System. No control deficiencies noted.
24. Mask Password	All passwords must be masked (i.e., made unreadable) when being entered to prevent unauthorized individuals from viewing the password.	White Oak determined that all passwords are masked when being entered into the Minimum Wage System. No control deficiencies noted.

25. Account Lockout	User and administrator accounts must be locked out after no more than: • 3 consecutive invalid logon attempts by that user during a 24-hour period for systems with a data protection categorization of High • 5 consecutive invalid logon attempts by that user during a one-hour period for systems with data protection categorization of Moderate • 10 consecutive invalid logon attempts by that user during a one-hour period for systems with data protection categorization of Low The account must remain locked for at least 30 minutes or until unlocked by an administrator.	White Oak determined that current lockout policy includes 5 invalid logon attempts results in an account being locked out for a duration of 5 minutes. The Department of Revenue has provided written approval of this implementation. No control deficiencies noted.
26. Inactivity Timeout	Sessions must be automatically locked after 15 minutes of inactivity. The user must be required to re-authenticate to reactivate the session.	White Oak determined that the session inactivity timeout is set to 15 minutes. No control deficiencies noted.
27. Multiple Sessions	Systems must prevent multiple concurrent active sessions for individual user accounts. System and application accounts must be limited to the number of concurrent sessions needed for their purpose and as documented in the system security plan.	White Oak determined that only one session is allowed at a time on the Minimum Wage System. No control deficiencies noted.
28. System Use Notification	A warning banner must be displayed prior to granting access to all internal networks, applications, databases, operating systems, workstations, servers, and network devices. Users must explicitly acknowledge the warning banner before being allowed access to the system. The system warning banner must include the following information: • The user is accessing a restricted government information system. • System usage may be monitored, recorded, and subject to audit. • Unauthorized use of the system is prohibited and may be subject to criminal and / or civil penalties. • Use of the system indicates consent to monitoring and recording.	White Oak determined the Minimum Wage System does utilize a warning banner prior to granting access for user account login. No control deficiencies noted.
29. Authorized Distribution	Users must ensure State data is only distributed to authorized personnel by: • Only allowing authorized personnel to view content on their screen. • Only including necessary and relevant information in system output such as reports and printouts. • Only distributing system output to individuals authorized to view all content.	White Oak determined State data is only distributed or allowed to be viewed by authorized personnel. No control deficiencies noted.

30. Database Access	All access to any database containing data with a data protection categorization of High (including access by applications, administrators, and all other users) must be restricted as follows: • All user access to, user queries of and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	White Oak determined that no database is installed or in-use on the Minimum Wage System. No control deficiencies noted.

Enterprise Security Logging and Monitoring Standard

Control Name	Control Detail	White Oak Observation
31. Logging	Implement automated logging on all systems to reconstruct the following events: • All actions taken by accounts with root or administrative privileges. • Access to all log data. • All log-in attempts. • Use of and changes to identification and authentication mechanisms – including but not limited to creation of new accounts and elevation of privileges – and all changes, addition, or deletions to accounts with root or administrative privileges. • Initialization, stopping, or pausing of the logs. • Creation and deletion of system-level objects.	White Oak determined the use of Windows events logging, Splunk, and FileSure for all logging activities on the Minimum Wage System. No control deficiencies noted.
32. Logging Individual User Access	Log all individual user access to data.	White Oak determined the use of Windows events logging, Splunk, and FileSure for logging all user activities on the Minimum Wage System. No control deficiencies noted.
33. Content of Log Records	Logged events must contain the following information: • User identification. • Type of event. • Timestamp. • Success or failure indication. • Origination of event. • Identity or name of affected data, system component, or resource.	White Oak determined the content of log files on the Minimum Wage System met the requirements listed. No control deficiencies noted.
34. Log Processing Failure	Systems must provide alerts in the event of a log processing failure.	White Oak determined that logs are reviewed quarterly and would determine if any processing failures occurred. No control deficiencies noted.
35. Log Review	Review the following using automated methods, where technically possible, at least daily: • All security events. • Logs of all systems that store, process or transmit data with a data protection categorization of High. • Logs of all systems that perform security functions including but not limited to firewalls, intrusion detection systems / intrusion prevent systems, and authentication servers.	All log files are collected quarterly and reviewed extensively of any identified issues. FRB MPLS actively ingests logs through the corporate Splunk configuration. No control deficiencies noted.
36. Clock Synchronization	Synchronize all system clocks to a designated internal time source that is accurate to the approved authoritative time source.	White Oak determined the Minimum Wage System is not networked and is utilizing the built-in clock. No control deficiencies noted.

37. Protection of Logs	Logs must be secured by: • Limiting viewing to those with a job-related need. • Protecting log files from unauthorized modifications. • Encrypting the logs in transit. • Requiring log configuration changes to be approved by authorized security personnel.	White Oak determined that logs are protected within the Minimum Wage system. No control deficiencies noted.
38. Retention of Logs	Retain log data for at least one year, with a minimum of three months immediately available for analysis. Log data for Federal Tax Information (FTI) must be retained for seven years.	No Federal Tax Information is being logged. Logs will be kept for 3 years by FRB MPLS. No control deficiencies noted.
39. Anti-Malware Software	Anti-malware software capable of detecting, removing, and protecting against all known types of malicious software on all systems commonly affected by malicious software and at critical points throughout the network. This software must: • Be actively running. • Prevent users from disabling or altering the software. • Generate event logs and continuously forward to an authorized central log server. • Automatically check for and install updates at least daily. • Perform scans of the system at least weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed. • Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection. • Be capable of addressing the receipt of false positives. • Be centrally managed.	**Medium Risk-Issue** White Oak reviewed this and determined that FRB MPLS does not meet the control objective. White Oak recommends FRB MPLS to ensure the installed anti-malware solution is updated properly during the implemented update windows. *FRB MPLS addressed this issue during the engagement and successfully implemented changes to ensure the anti-malware software is updated per the proper window.*
40. Anti-Malware Review	For systems not commonly affected by malicious software, perform evaluations at least annually to identify and evaluate evolving malware threats in order to confirm whether such systems do not require anti-malware software.	FRB MPLS has implemented anti-malware on the Minimum Wage System. No control deficiencies noted.

Enterprise Physical and Environmental Security Standards

Control Name	Control Detail	White Oak Observation
41. Labeling	Systems and media must be labeled to indicate the handling and access requirements.	White Oak determined the Minimum Wage System, along with a primary and secondary hard drive have been labeled properly. No control deficiencies noted.

42. Secure Storage of Paper and Electronic Media	Paper and electronic media containing State data must be kept under the immediate protection and control of an authorized personnel or securely locked up.	**Low Risk-Issue** White Oak determined that FRB MPLS should implement additional containment around paper media in the form of handwritten project notes created by the approved project researchers within the workstation area. FRB MPLS could utilize existing locking cabinets to contain paper media while the room is unoccupied.
43. Media Inventory	Electronic media containing State data must be inventoried at least annually. Inventories must be documented and any discrepancies with previous inventories must be investigated and communicated to the security incident response team.	FRB MPLS will inventory the Minimum Wage System annually. The first inventory has yet to occur of the system. No control deficiencies noted.
44. Media Transport	The transport of any kind of paper or electronic media containing State data must be strictly controlled, including the following: • Categorize the media based on the data it contains. • Send the media by secured courier or other secure delivery method that can be accurately tracked. • Monitor the transport to ensure that each shipment is properly and timely received and acknowledged. • Document the transport of all media. • Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). • Restrict the activities associated with the transport of media to authorized personnel. • Maintain accountability for media during transport outside of secured areas. • All electronic media must be encrypted.	The media transportation of State data follows multiple strict guidelines within FRB MPLS. All data is encrypted and proper accountability is performed. No control deficiencies noted.

45. Secure Disposal of Electronic Media	Media must be securely disposed of when it is no longer needed for business or legal reasons and in accordance with record retention requirements as follows: • Review and approve media to be sanitized to ensure compliance with business, legal, and records retention requirements. • Sanitize or destroy all media prior to disposal, release out of State control or reuse. • Ensure the sanitization or destruction is witnessed or carried out by authorized personnel. • Verify the media sanitization or destruction was successful. • Document sanitization and destruction actions including: o Personnel who reviewed and approved sanitization or disposal actions. o Types of media sanitized. o Sanitization methods used. o Date and time of the sanitization actions. o Personnel who performed the sanitization. o Verification actions taken. o Personnel who performed the verification. o Disposal action taken. • Provide the business a certificate of destruction confirming disposition of the media.	White Oak reviewed FRB MPLS's disposal process and determined it meets all requirements. No control deficiencies noted.

46. Physical Barriers	Areas of the facility containing State systems and data must be physically separated from other areas of the facility by: • Separating nonpublic areas from public areas with physical barriers (e.g., walls, doors, turnstiles, etc.) and identifying areas as nonpublic with prominent postings. • Separating sensitive areas such as data centers, network closets, and areas storing or processing data from other areas of the facility using physical barriers. • Minimizing the number of entrances to nonpublic and sensitive areas. • Controlling entry and exit points to nonpublic and sensitive areas of the facility using physical access control systems / devices and / or guards. • Restricting physical access to wireless access points, gateways, handheld devices, networking / communications hardware, and telecommunication lines.	Multiple physical barriers are implemented to restrict access to the Minimum Wage System to very limited individuals at FRB MPLS. No control deficiencies noted.

47. Physical Access Control	Physical access to nonpublic and sensitive areas must be controlled by: • Developing, approving, and maintaining a list of individuals with authorized access to nonpublic and sensitive areas of the facility. This list must include: o Name of individual. o Agency or department name. o Name and contact information of agency point of contact. o Purpose for access. • Reviewing and updating the access list detailing authorized access by individuals at least every six months for data centers and at least annually for all other areas. • Authorizing access to nonpublic and sensitive areas based on the individual's job function. • Prohibiting "piggybacking" or "tailgating" into nonpublic or sensitive locations. • Issuing badge access, keys, and / or combinations only to authorized individuals. • Revoking access when no longer needed and ensuring all physical access mechanisms, such as keys, access cards, etc., are returned, changed, and / or disabled. • Requiring the use of two factor of authentication for physical access to data centers. • Requiring the inspection of all bags and items entering data centers and limiting access to only those items that are needed to perform work. • Requiring the completion of required background checks and training prior to granting access to data centers.	Physical access to the room housing the Minimum Wage System has been recently limited to strictly researchers. Other personnel require prior approval and being escorted by researchers. No control deficiencies noted.

48. Physical Access Monitoring	Video cameras and / or access control systems (e.g., badge readers, smart cards, biometrics, etc.) must be used to monitor and track all physical access attempts to nonpublic and sensitive areas. Video and / or access control logs must: • Capture the following information: o The owner of the access control device requesting access and / or the identity of the individual requesting access. o The success or failure of the request. o The data and time of the request. • Be reviewed at least monthly and correlated with other entries. • Unauthorized access must be reported to the security incident response team for investigation. • Stored for at least 90 days for data centers and areas containing data with data protection categorization of High. • Be monitored 24 hours per day, 7 days per week by trained personnel who respond to potential incidents. • Be analyzed by automated mechanisms to recognize potential intrusions and initiate designated response actions.	Multiple video cameras are implemented to capture initial access to the building and specific areas of the building housing the Minimum Wage System, including a camera positioned directly outside of the Minimum Wage Secure Room door. The cameras are monitored 24 hours a day by trained personnel. Badge readers are utilized to access all areas of the building. The access logs are reviewed frequently. No control deficiencies noted.
49. Physical Access Device Management	Keys, combinations, and other physical access devices must be protected by: • Storing keys, combinations, and other physical access devices in a secure location. • Inventorying and reconciling all keys and other physical access devices at least annually. • Changing combinations at least annually and when an employee who knows or has access to them no longer has a need to access the area, room, or container. • Only giving keys, combinations, and other physical access devices to those who have a frequent need to have access to the area, room, or container.	Physical key to the Minimum Wage System room is protected within a secure location with limited access. No control deficiencies noted.

50. Visitor Access	Visitors to nonpublic or sensitive areas must be: • Authorized before entering. • Escorted and monitored at all times within nonpublic or sensitive areas. • Identified by examining government issued photo identification (e.g., state driver’s license or passport) for data centers and areas containing Federal Tax Information. • Given a badge or other identification that: o Expires no later than the end of the visit. o Visibly distinguishes the visitors from authorized personnel. o Is returned before leaving the facility or at the data of expiration.	Visitors are not granted individual access to the room or to the Minimum Wage System. Any visitors must have prior approval and be escorted by authorized individuals to gain access to the Minimum Wage System room. No control deficiencies noted.
51. Visitor Log	A visitor log must be used to maintain a physical audit trail of all visitor activity to nonpublic and sensitive areas. This visitor log must: • Be retained for a minimum of 12 months. • Be closed out at the end of each month and reviewed by management. • Contain the following information: o Name of the visitor. o Organization of the visitor. o Signature of the visitor (electronic or physical). o Form of identification reviewed (if required). o Date of access. o Time of entry and departure. o Purpose of visit. o Name and organization of authorized escort.	A visitor log is generated upon entry to the FRB MPLS building. An authorized FRB MPLS escort is with visitors at all times. No control deficiencies noted.

52. Maintenance Personnel Access	Physical access for cleaning, security, and maintenance personnel must be controlled by: • Maintaining a list of authorized maintenance organizations or personnel. This list must be updated at least every 6 months and include: o Name of vendor / contractor. o Name and phone number of State point of contact authorizing access. o Name and contact information of vendor point of contact. o Address of vendor / contractor. o Purpose and level of access. • Ensuring that non-escorted maintenance and cleaning personnel have completed the same training, screening, and approval as authorized employees. • Designating State personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not have the required access authorizations.	FRB MPLS requires all maintenance personnel to have prior approval of any required access to the Minimum Wage System room. All access granted will be escorted by authorized personnel. No control deficiencies noted.
53. Facilities Maintenance Records	Repairs and modifications to the physical components of a facility which are related to security (for example, door hinges and handles, walls, doors, and locks) must be approved and documented.	Any repairs or modifications are submitted and approved through the proper approval process. All access to the Minimum Wage System room is monitored and escorted by authorized personnel. No control deficiencies noted.