US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

DEPARTMENT OF VETERANS AFFAIRS

Evaluation of the May 2023 Power Outage at the Hines Information Technology Center in Illinois

Review	23-03063-164	May 29, 2024

BE A
VOICE FOR
VETERANS
REPORT WRONGDOING
vaoig.gov/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Executive Summary

At the request of the Secretary of Veterans Affairs, the VA Office of Inspector General (OIG) conducted this review to evaluate a power outage that occurred at the Hines Information Technology Center on May 4, 2023. The outage lasted approximately 22 hours and adversely affected more than 10,000 VA employees nationwide, preventing them from accessing critical VA data and systems such as compensation, pension, and education benefits applications. The objective of this review was to evaluate the Hines Information Technology Center's access controls and contingency planning to determine their role in the power outage and resulting impact to VA employees.

What the Review Found

The OIG found that the Hines Information Technology Center electrical power infrastructure design includes a circuit breaker that functions as a master power switch between the uninterruptible power supplies and the information technology equipment. The OIG also determined that this design did not meet a power distribution standard for VA core data centers, which require redundant distribution paths between the uninterruptible power supplies and the information technology equipment.[1] Consequently, when the circuit breaker was activated on May 4, 2023, by an authorized employee, it interrupted the flow of electricity going to the data center equipment and critical applications hosted at the facility.[2] Unless this is updated, the Hines center will remain at risk of a similar event.

Furthermore, the OIG noted that the circuit breaker did not have a protective covering to prevent it from being activated or a warning label indicating the breaker's function, which ultimately contributed to the power interruption. While the OIG did not evaluate the consistent implementation of physical security controls across all VA data centers, it did tour the Austin Information Technology Center as part of this review and noted an additional feature covering its circuit breakers. Like the Hines facility, the Austin Information Technology Center has circuit breakers supporting the electrical system; however, the circuit breakers have plastic covers with lids that are affixed to the breaker panel with screw fasteners. To activate that breaker, a user would need to lift the lid, open the cover, and then activate the switch. While this device does not inhibit access to the switch, it adds a step that may be effective in preventing accidental activation of the breaker. VA guidance does not require using protective circuit breaker covers at the data centers.[3] The OIG determined that placing a protective covering over the circuit breaker

[1] VA Office of Information and Technology (OIT), *Infrastructure Standard for Telecommunications Spaces*, ver. 3.0, August 21, 2020.

[2] VA OIG's Office of Investigations concluded that there was not sufficient evidence to establish that the employee had intent to commit a federal crime but did not make a final determination on whether the actions were accidental.

[3] VA OIT, *Infrastructure Standard for Telecommunications Spaces*.

and explicit warning labels might have prevented the accidental disruption of electricity at the Hines facility.

The Hines Information Technology Center also did not have a detailed information system contingency plan to guide staff in the recovery of facility information systems following a power outage. Consequently, when the power outage occurred, engineering staff did not coordinate with the Office of Information and Technology (OIT), and OIT stated there were issues with the prioritization of network devices. The power outage prevented VA employees from accessing critical VA data and applications such as compensation, pension, and education benefits applications.

While the Hines Information Technology Center's shared infrastructure contingency plan broadly discusses recovering from a power outage, it outlines no specific procedures to guide staff in restoring critical systems and network devices, as required by the National Institute of Standards and Technology (NIST).[4] The OIG concluded that having a detailed contingency plan to define specific recovery procedures would have allowed staff to more efficiently restore power, network infrastructure, and critical applications, and would have caused less downtime for the facility and end users.

Although the Hines center is configured with VA standard physical access controls, a protective covering over the main circuit breaker and an explicit warning label indicating the breaker's function could have prevented the mistaken activation of the breaker. Because the circuit breaker activated during this event functions as a master power switch between the uninterruptible power supplies and the information technology equipment, VA remains at risk of a similar event at the facility that could disrupt critical systems. These power outages could cause veterans and their families to experience significant delays in receiving important services. Therefore, OIT should implement adequate physical security controls and develop a detailed contingency plan to reduce system downtime in the event of a power outage.

What the OIG Recommended

The OIG recommended that the assistant secretary for information and technology consider taking appropriate steps to implement redundant distribution paths between the uninterruptible power supplies and the information technology equipment at the Hines Information Technology Center. The OIG also recommended considering using a protective covering with a warning label for the circuit breaker at the Hines Information Technology Center and updating the physical security controls policy to require protective covers with warning labels for all circuit breakers at VA data centers. The OIG also recommended that the assistant secretary implement improved information system contingency planning and recovery procedures, including annual power

[4] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

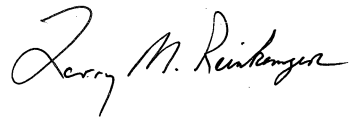
outage exercises, to ensure facility staff can restore network devices and mission-critical systems in a timely manner.

VA Management Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with all five recommendations and submitted a responsive action plan, which included milestone dates for planned corrective actions for all recommendations. The full text of the assistant secretary's response is included in appendix C.

In response to the recommendations, the assistant secretary reported OIT will conduct a feasibility study to evaluate the cost and benefit of redundant distribution paths, install a protective covering over the circuit breaker and add a warning label, update physical security policies, review and update the Hines Information Technology Center information system contingency plans, and implement annual testing of contingency plans and restoration procedures with an emphasis on power-loss events.

The OIG will monitor the implementation of all five recommendations and close them when VA provides sufficient evidence demonstrating progress in addressing the issues identified.



LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

FISCAM	Federal Information Security Controls Audit Manual
FISMA	Federal Information Security Modernization Act
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
VBA	Veterans Benefits Administration

Introduction

At the request of the Secretary of Veterans Affairs, the VA Office of Inspector General (OIG) conducted this review to evaluate a power outage that occurred at the Hines Information Technology Center on May 4, 2023. The outage lasted approximately 22 hours and adversely affected more than 10,000 VA employees, preventing them from accessing critical VA data and systems such as compensation, pension, and education benefits applications.

The objective of this review was to evaluate the Hines Information Technology Center's access controls and contingency planning to determine their role in the power outage and subsequent effects on VA employees. Both the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) provide criteria to establish minimum requirements and controls for federal information security programs.[5] Although the findings and recommendations in this report are specific to the Hines center, other VA facilities could benefit from reviewing this information and considering the recommendations.

Hines Information Technology Center

The Hines Information Technology Center (Hines center) is located on the VA hospital campus in Hines, Illinois (figure 1).

[5] Office of Management and Budget (OMB), *Security of Federal Automated Information Resources*, app. 3 in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; and NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, last updated December 10, 2020.

Figure 1. *Hines Information Technology Center.*
Source: Hines Security Specialist, August 1, 2023.

Over 220 VA employees and numerous contractor staff at the Technology Center support operations of applications and systems for the Veterans Benefits Administration (VBA). The Hines center is owned and maintained by VA and was constructed to accommodate VA's centralized information technology, equipment, and functions, including the following:

- The development, maintenance, and processing of all compensation, pension, and education benefits applications.
- The operation and maintenance of information technology hardware and peripheral equipment that supports 57 VBA regional offices, as well as a telecommunications network that supports Benefits Delivery Network processing.[6]
- The development, installation, and maintenance of system software and operating systems that support VBA's local and wide-area networks.

[6] Benefits Delivery Network is VA's main processing system for certain awards and related actions. It generates the payment information that is sent to the US Department of the Treasury, where benefit checks are produced. It also contains the master record files for veterans and other beneficiaries.

Power Outage Event

On May 4, 2023, a Hines engineer who was authorized to be in the electrical room turned the handle to the data center's main power circuit breaker, interrupting power to the facility.[7] The circuit breaker did not have a protective covering over the switch or an explicit warning label indicating that the breaker-controlled power at the data center. The system outage lasted approximately 22 hours and adversely affected more than 10,000 VA employees nationwide, preventing them from accessing critical VA data and systems such as compensation, pension, and education benefits applications.

[7] VA OIG's Office of Investigations concluded that there was insufficient evidence to determine that the employee intended to interrupt VA system functionality but did not make a final determination regarding whether the physical actions triggering the interruption were accidental.

Results and Recommendations

Finding: Certain Facility Physical Access Controls and Contingency Planning Controls Can Be Improved

Certain access and contingency planning controls can be improved at the Hines Information Technology Center. The team based this finding on the following:

- **Access controls.** The center's main circuit breaker was activated by an authorized employee. There was no physical security control in place to prevent such action. Although the center has controls to prevent unauthorized access to the electrical room, improvements could be made to avoid power losses to the data center and mission-critical systems.
- **Data center redundancy.** The electrical power infrastructure design includes a circuit breaker that functions as a master power switch between the uninterruptible power supplies and the information technology equipment. However, this design did not meet a current power distribution standard for VA core data centers, which requires redundant distribution paths between the uninterruptible power supplies and the information technology equipment.[8] Consequently, when the circuit breaker was activated in May 2023, it interrupted the flow of electricity going to the data center equipment and critical applications hosted at the facility. Unless this is updated, the Hines center will remain at risk of a similar event.
- **Contingency planning controls.** The Information Systems Contingency Plan did not provide sufficient detail to guide staff in the recovery of facility information systems following a power outage. Consequently, when the power outage occurred, center staff explained that they did not prioritize the restoration of systems and services.

Without having adequate physical protection over the electrical system's circuit breakers, VA is at risk of repeated power losses at facilities, which could disrupt critical systems and veterans' access to necessary services. While the OIG found the current physical security controls sufficient for preventing unauthorized access to the electrical room, the team identified opportunities for VA to better protect its systems from a potential recurrence of this event. To mitigate this risk, OIT should implement adequate physical security controls over circuit breakers and develop a detailed contingency plan to reduce system downtime during a power outage.

[8] VA Office of Information and Technology (OIT), *Infrastructure Standard for Telecommunications Spaces*, ver. 3.0, August 21, 2020. "Redundant" in this case means that there is more than one distribution path, and they are independent.

What the OIG Did

The OIG reviewed physical access and contingency planning controls at the Hines Information Technology Center. The OIG interviewed OIT personnel and facility staff to gain a better understanding of the power outage and events that occurred on May 4, 2023. The OIG reviewed federal directives, VA policy, and industry best practices that applied to data center operations. Appendix A contains more information on the directives and standards; appendix B describes the review scope and methodology.

Access Controls

According to federal guidance for information system control audits, access controls provide reasonable assurance that access to computer resources (such as data, equipment, and facilities) is restricted to authorized individuals and include effective protection of information system boundaries, identification and authentication mechanisms, authorization controls, protection of sensitive system resources, audit and monitoring capability—including incident handling—and physical security controls.[9] The inspection team evaluated one access control critical element: establishing adequate physical security controls. Physical security access controls involve restricting access to computer resources and protecting them from intentional or unintentional loss or impairment.[10]

Data Center Redundancy

VA core data centers are planned to hold a redundancy rating of 3 as established by the Telecommunications Industry Association's Telecommunications Infrastructure Standard for Data Centers.[11] For example, electrical distribution from the uninterruptible power supply to the information technology equipment should be redundant. However, the circuit breaker activated at the Hines Information Technology Center functions as a master power switch between the uninterruptible power supplies and the information technology equipment. Data center personnel stated that the placement of the circuit breaker is necessary to support the design of the electrical systems at the Hines facility.

Physical Security Controls Were Generally Adequate but with Critical Exceptions

The OIG assessed the current physical security controls and found them sufficient for preventing unauthorized access to the electrical room. However, the center did not implement an effective

[9] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G, February 2009.

[10] GAO, *FISCAM*.

[11] VA OIT, *Infrastructure Standard for Telecommunications Spaces*; and ANSI/TIA-942-B-2017, *Telecommunications Infrastructure Standard for Data Centers*, July 12, 2017.

physical control to prevent the activation of a circuit breaker that caused an inadvertent outage at the data center. Specifically, the OIG noted that the circuit breaker did not have a protective covering over the switch or an explicit warning label indicating that the breaker switch controls all power at the data center. Figure 2 is a picture of the unprotected circuit breaker.

Figure 2. *Unprotected circuit breaker at Hines Information Technology Center.*

Source: OIG, July 11, 2023.

While the OIG did not evaluate whether VA consistently implemented similar physical security controls across all its data centers, the review team did tour the Austin Information Technology Center twice and found that the facility uses protective coverings over its circuit breakers. Like the Hines facility, the Austin Information Technology Center had circuit breakers supporting the power system; however, these circuit breakers had plastic covers affixed to the breaker panel with screw fasteners. To activate those breakers, a user would need to lift the lid, open the cover, and then turn the switch handle. Figure 3 shows the protective covering in use at the Austin facility.

Figure 3. *Protected circuit breaker at the Austin Information Technology Center.*

Source: OIG, January 8, 2024.

Although VA policy does not require that facilities use protective coverings over circuit breakers, the Austin center's use of plastic covers provides an additional measure of security. Such a cover does not prevent intentional activation of the breaker, but a cover with a specific warning adds a layer of physical security that can help prevent inadvertent shutoffs of power distribution equipment. In particular, the cover requires a deliberate step to reach the breaker, and the warning identifies the consequences of activating the breaker. Without having adequate physical protection over the Hines center circuit breaker, VA is at risk of inadvertent power losses at the facility, which could disrupt critical systems and veterans' access to necessary services.

Contingency Planning Controls

According to federal guidance for information system control audits, contingency planning provides reasonable assurance that information resources are protected, and the risk of unplanned interruptions is minimized.[12] Contingency planning also allows for recovery of critical operations if interruptions occur. The inspection team evaluated four critical elements for contingency planning:[13]

- Assess the criticality and sensitivity of computerized operations and identify supporting resources.
- Take steps to prevent and minimize potential damage and interruption.
- Develop and document a comprehensive contingency plan.
- Periodically test the contingency plan and adjust it as appropriate.

[12] GAO, *FISCAM*.

[13] GAO, *FISCAM*.

Hines Information Technology Center Did Not Have a Detailed Contingency Plan

The OIG found that the Hines Information Technology Center's contingency plan lacked sufficient detail to guide staff in the recovery of all facility information systems following a power outage. While a contingency plan should provide steps to restore data center services, the Hines center's plan does not provide the specific procedures to guide staff in restoring critical systems in the event of a power disruption.[14] Additionally, the plan does not define essential business functions, contain restoration priorities, or have recovery procedures for systems and network devices hosted at the facility in accordance with NIST guidance. Consequently, when the power outage occurred, engineering staff did not coordinate with OIT, and OIT stated there were issues with the prioritization of network devices. The scale of the outage—lasting approximately 22 hours and affecting more than 10,000 employees—reflects the importance of having an adequate contingency plan to mitigate the impact of a power outage.

Restoration Responsibility Was Unclear and Procedures Untested

While the facility contingency plan provided information needed for system recovery, including roles and responsibilities, the plan provided conflicting responsibilities for personnel during the facility and system restoration process. For instance, VA's Knowledge Service provides guidance for defining roles and responsibilities and designates the system owner as responsible for developing and documenting the facility contingency plan. However, the system authorization to operate accreditation package assigns contingency plan responsibility to Business Continuity Program coordinators.[15] Moreover, the Hines center's contingency plan makes the contingency plan director or the deputy director of the systems service line responsible for the contingency plan, contrary to the VA Knowledge Service policy above. Without clearly defined business functions and system restoration priorities, future power outages will result in delays when restoring critical information system and network components.

The Hines center's shared infrastructure contingency plan also requires facility staff to ensure that power is only restored once staff have completed a power outage assessment and have determined that it is safe to restore power. However, facility staff did not follow these requirements. Specifically, data center power was restored before coordinating with infrastructure operations staff, resulting in network devices and systems being restored out of sequence, thereby increasing the length of the restoration process. Although the contingency plan is tested annually, responding to a simulated power loss was not part of the exercise. As a result,

[14] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

[15] OIT issues a system authorization to operate that explicitly accepts the risk to agency operations, assets, and individuals based upon the implementation of security and privacy controls.

personnel were not prepared to manage an actual power outage as required by the contingency plan.

Conclusion

The Hines center has not implemented effective physical controls to prevent the inadvertent activation of a circuit breaker. Although the center is configured with VA standard physical access controls, installing a protective covering over the circuit breaker and an explicit warning label indicating the breaker's function might have prevented the power outage at the facility. While the protective covering would not deter someone with malicious intent from tripping the circuit breaker, it might prevent an individual from inadvertently cutting power to the facility. Without having some level of physical protection over the circuit breaker, veterans and VA are at risk of experiencing this service disruption again due to power loss at the center, potentially delaying important services to veterans and their families.

The Hines data center design does not meet a current power distribution standard for VA core data centers, which requires redundant distribution paths between the uninterruptible power supplies and the information technology equipment.[16] Consequently, the circuit breaker activated during this event acted as a master power switch between the uninterruptible power supplies and the information technology equipment. Unless this is updated, the Hines center will remain at risk of a similar event.

Without clearly defined contingency plan business functions and restoration priorities, delays will occur during the recovery of critical information system components at the Hines center. Having a detailed contingency plan that defines specific recovery procedures would have allowed center staff to efficiently restore data center services, resulting in less downtime for the facility and end-user operations. By not simulating a power loss during the testing of the contingency plan, personnel were not aware of their responsibilities when restoring network services and critical systems during power outages.

Recommendations 1–5

The OIG made the following recommendations to the assistant secretary for information and technology and the chief information officer:

1. Consider taking appropriate steps to implement redundant distribution paths between the uninterruptible power supplies and the information technology equipment at the Hines Information Technology Center.

[16] VA OIT, *Infrastructure Standard for Telecommunications Spaces*.

2. Implement steps to prevent the inadvertent activation of the main circuit breaker at the Hines Information Technology Center, such as installing a protective covering over the circuit breaker with an explicit warning label indicating the breaker's function to help prevent power outages at the facility.
3. Implement steps to prevent the inadvertent activation of circuit breakers at all VA data centers, such as updating the physical security controls policy to require protective covers and explicit warning labels.
4. Update the Hines Information Technology Center information system contingency plan to help ensure the efficient restoration of data center power and critical applications in the event of a power outage.
5. Implement annual testing of Hines Information Technology Center contingency and restoration procedures following a power loss to ensure all stakeholders are aware of their responsibilities in accordance with revised information system contingency plan procedures.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with all five recommendations and submitted a responsive action plan, which included milestone dates for planned corrective actions for all recommendations. The full text of the assistant secretary's response is included in appendix C.

Regarding recommendation 1, the assistant secretary reported OIT will conduct a feasibility study to evaluate the cost and benefit of redundant distribution paths between the uninterruptible power supplies and the Hines Information Technology Center. For recommendation 2, OIT will install a protective covering over the circuit breaker and add a warning label indicating the breaker's function. Regarding recommendation 3, OIT will update physical security policies to require a protective covering over circuit breakers, along with warning labels. The updated policies will require sites without these protective measures in place to implement them. For recommendation 4, OIT will review and update the Hines Information Technology Center information system contingency plans based on lessons learned from the 2023 power outage. Specifically, updates to the contingency plans will emphasize procedures for notifying impacted stakeholders and include appropriate sequencing of equipment and application start-up procedures. To address recommendation 5, OIT will implement annual testing of contingency plans and restoration procedures with an emphasis on power-loss events. Implementation of contingency plans will include informing and including all stakeholders in testing, as well as emphasizing appropriate sequencing and coordination for equipment restarts.

OIG Response

The assistant secretary for information and technology and chief information officer's planned corrective actions are responsive to the intent of all recommendations. The OIG will monitor the implementation of all five recommendations and will close them when VA provides sufficient evidence demonstrating progress in addressing the issues identified.

Appendix A: Background

Federal Information System Controls Audit Manual

The Government Accountability Office developed the *Federal Information Security Controls Audit Manual* (FISCAM) to provide auditors and information system control specialists a methodology for evaluating the confidentiality, integrity, and availability of information systems.[17] FISCAM groups controls into categories that have similar risks. To assist auditors in evaluating information systems, FISCAM maps its control categories to the National Institute of Standards and Technology's (NIST) controls. FISCAM lists six critical elements for access control:

- **Boundary protection.** Pertains to the protection of a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction.
- **Identification and authentication.** Identification is the process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. Authentication is the verification of the identity of a user, process, or device.
- **Authorization.** Determine what users can do, such as granting access to various resources, and depend on valid identification and authentication controls.
- **Sensitive system resources.** Designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption and certificate management.
- **Audit and monitoring.** Involves the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during and after an attack.
- **Physical security.** Restricts access to computer resources and protects them from loss or impairment. These controls include guards, gates, and locks, and environmental controls such as smoke detectors, fire alarms, and extinguishers, and uninterruptible power supplies.

[17] Government Accountability Office, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G, February 2009.

Federal Information Security Modernization Act (FISMA) of 2014

The following are the stated goals of FISMA:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks.
- Provide for development and maintenance of minimum controls required to protect federal information and information systems.
- Provide a mechanism for improved oversight of federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions.
- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[18]

FISMA also requires an annual independent assessment of each agency's information security program to determine its effectiveness, which must be conducted by the agency's inspector general or an independent external auditor.[19] The VA Office of Inspector General (OIG) completes the annual FISMA evaluation through a contracted external auditor and provides oversight of the contractor's performance.

[18] *Federal Information Security Modernization Act of 2014* (FISMA), 44 U.S.C. § 3551.
[19] FISMA, 44 U.S.C. § 3555.

Appendix B: Scope and Methodology

Scope

The review team conducted its work from July 2023 through February 2024. The team evaluated physical security access controls and contingency planning controls relevant to the outage that occurred at the Hines Information Technology Center in accordance with FISMA, NIST security guidelines, and VA's information security policy.

Methodology

To accomplish the objective, the evaluation team examined relevant laws, policies, and industry best practices. The team also inspected the facility and systems for compliance with VA physical access and contingency planning controls. The team interviewed VA personnel responsible for the Hines center's information security and operations, and facility management. The OIG toured the Austin Information Technology Center to evaluate whether consistent physical access controls were implemented at two VA data centers. Finally, the team analyzed interview results and evaluated business processes to identify policy violations and potential threats to security.

Internal Controls

The evaluation team determined that internal controls were significant to the evaluation objectives. When planning for this evaluation, the team identified potential information system controls that would significantly affect the recovery of network devices and critical applications in the event of a power outage. Specifically, the team used applicable national and department policies as a guide to help develop evidence requests and applicable interview questions for facility personnel. Specifically, the team determined that the control component "Control Activities," the control principle "Design of Appropriate Types of Control Activities for the Information System," and specific controls over physical security and contingency planning were significant to our objectives.

Fraud Assessment

The evaluation team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the audit objectives, could occur during this evaluation. The team exercised due diligence in staying alert to any fraud indicators. The OIG did not identify any instances of fraud or potential fraud during this audit.

Data Reliability

The evaluation team did not use generated computer-processed data.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.*

Appendix C: VA Management Comments

Department of Veterans Affairs Memorandum

Date: April 12, 2024

From: Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Evaluation of the May 2023 Power Outage at the Hines Information Technology Center in Illinois, Project Number 2023-03063-AE-0121 (VIEWS 11547447)

To: Assistant Inspector General for Audits and Evaluations (52)

1. Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, *Evaluation of the May 2023 Power Outage at the Hines Information Technology Center in Illinois* (Project Number 2023-03063-AE-0121).

2. The Office of Information and Technology (OIT) submits the attached written comments, along with a target completion date for each of the OIG's recommendations to the Department.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology

Comments on Office of Inspector General Draft Report,

Evaluation of the May 2023 Power Outage at the Hines Information Technology Center in Illinois, Project Number OIG-2023-03063-AE-0121

(VIEWS 11547447)

Recommendation 1: Consider taking appropriate steps to implement redundant distribution paths between the uninterruptible power supplies and the information technology equipment at the Hines Information Technology Center.

Comments: Concur.

The Office of Information and Technology (OIT) will conduct a feasibility study to evaluate the cost and benefit of redundant distribution paths between the uninterruptible power supplies and the Hines Information Technology Center.

Expected Completion Date: September 30, 2024.

Recommendation 2: Implement steps to prevent the inadvertent activation of the main circuit breaker at the Hines Technology Center, such as installing a protective covering over the circuit breaker with an explicit warning label indicating the breaker's function to help prevent power outages at the facility.

Comments: Concur.

OIT will install a protective covering over the circuit breaker and add a warning label indicating the breaker's function.

Expected Completion Date: June 30, 2024.

Recommendation 3: Implement steps to prevent the inadvertent activation of circuit breakers at all VA data centers, such as updating the physical security controls policy to require protective covers and explicit warning labels.

Comments: Concur.

OIT will update physical security policies to require a protective covering over circuit breakers, along with warning labels. The updated policies will require sites without these protective measures currently place to implement them.

Expected Completion Date: September 30, 2024.

Recommendation 4: Update the Hines Information Technology Center information system contingency plan to help ensure the efficient restoration of data center power and critical applications in the event of a power outage.

Comments: Concur.

OIT will review and update the Hines Information Technology Center information system contingency plans based on lessons learned from the 2023 power outage. Specifically, updates to the contingency plans will emphasize procedures for notifying impacted stakeholders and include appropriate sequencing of equipment and application startup procedures.

Expected Completion Date: December 31, 2024.

Recommendation 5: Implement annual testing of Hines Information Technology Center contingency and restoration procedures following a power loss to ensure all stakeholders are aware of their responsibilities in accordance with revised information system contingency plan procedures.

Comments: Concur.

OIT will implement annual testing of contingency plans and restoration procedures with an emphasis on power loss events. Implementation of contingency plans will include informing and including all stakeholders in testing, as well as emphasizing appropriate sequencing and coordination for equipment restarts.

Expected Completion Date: March 30, 2025.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Review Team	Michael Bowman, Director Jack Henserling George Ibarra Justin Skeen Brandon Zahn
Other Contributors	Clifford Stoddard Andrew Eichner Nate Landkammer Andrew Tuzzolino

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Director, Hines Information Technology Center

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.vaoig.gov.