STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-018
August 2019

AGENCY FOR PERSONS WITH DISABILITIES

Information Technology General Controls

Sherrill F. Norman, CPA
Auditor General

Director of the Agency for Persons with Disabilities

The Agency for Persons with Disabilities is created by Section 20.197, Florida Statutes, as a separate budget entity within the Department of Children and Families for administrative purposes only. The head of the Agency is the Director who is appointed by the Governor and subject to confirmation by the Senate. Barbara Palmer served as Director during the period of our audit.

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

AGENCY FOR PERSONS WITH DISABILITIES

Information Technology General Controls

SUMMARY

This operational audit of the Agency for Persons with Disabilities (Agency) focused on evaluating selected information technology (IT) general controls and included follow up on Finding 5 included in our report No. 2016-071. Our audit disclosed the following:

Finding 1: The Agency's *Information Security Program Policy* did not encompass or reference significant aspects of a comprehensive information security program.

Finding 2: Security awareness training for Agency employees was not always completed timely.

Finding 3: Agency computer security incident response processes need improvement.

Finding 4: The Agency did not timely disable the network access privileges for some former employees.

Finding 5: Agency policies and procedures for periodic reviews of access privileges need improvement.

Finding 6: Certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management need improvement.

BACKGROUND

Pursuant to State law,[1] the Agency for Persons with Disabilities (Agency) is responsible for the provision of services to persons with developmental disabilities under State law,[2] including the operation of all State institutional programs and the programmatic management of Medicaid waivers established to provide services to persons with developmental disabilities. The Agency works with local communities and private providers to support people who have developmental disabilities in living, learning, and working in their communities.

The mission of the Office of Information Technology (OIT) within the Agency is to align with the Agency's strategic goals and initiatives; provide effective, efficient, reliable, and cost-conscious technology solutions to Agency staff so they can focus on client needs, deliver results, and achieve the Agency's mission; maintain the privacy, security, and integrity of client, employee, and citizen data; manage projects using industry-standard methodologies while delivering projects on time and within budget; and provide customer focused, responsive technical support services.

[1] Section 20.197(3), Florida Statutes.

[2] Chapter 393, Florida Statutes.

FINDINGS AND RECOMMENDATIONS

Finding 1: Information Security Program

Effective IT security controls include documented, management approved policies and procedures that describe the information security program for providing security for the information and information systems that support the operations and assets of the agency. Agency for State Technology (AST)[3] rules[4] require each agency to establish an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process; a Computer Security Incident Response Team (CSIRT); and a disaster recovery program that aligns with agency's continuity of operations plan. AST rules[5] also require each agency to develop procedures to protect information systems and assets by establishing a configuration change control process to manage upgrades and modifications to existing IT resources and to ensure that backups of information are conducted, maintained, and tested.

The Agency's *Information Security Program Policy*[6] (*Policy*) states the Agency will establish and maintain an information security program to administer the Agency's information security matters, and to implement cost-effective safeguards to address risks to the data, information, and information technology resources of the Agency. Our evaluation of the *Policy*, last updated on October 22, 2012, disclosed that the *Policy* did not encompass or reference significant aspects of a comprehensive information security program such as relevant security policies, procedures, standards, and guidelines, an information security awareness program, or a CSIRT. Our audit procedures also disclosed that, as of April 5, 2019, the Agency did not have:

- Policies and procedures for security awareness training and on-going education and reinforcement of security practices.
- A procedure for identifying and categorizing security incidents including the types of incidents defined in each category. The *Information Security Incident and Breach Response Policy*,[7] which outlined the procedures to follow when a security incident or breach is discovered or suspected, did not include a requirement or guidance for assigning a risk categorization to security incidents.
- Documented policies and procedures governing the back up of data on Agency-managed servers including frequency for performing backups, backup retention periods, and recoverability testing.
- Documented procedures for firmware patches for high-risk network devices and network servers including the timeframe for applying patches, patch analysis processes, and the backout steps to be performed in the event an applied patch needs to be reversed.

[3] Effective July 1, 2019, Chapter 2019-118, Laws of Florida, creates the Division of State Technology within the Department of Management Services (DMS) and transferred the existing powers, duties, functions, personnel, records, property, and funds of the Agency for State Technology (AST) to the Division of State Technology.

[4] AST Rule 74-2.002(1)(f)8.c., Florida Administrative Code. Effective July 1, 2019, AST Rules, Chapter 74-2, Florida Administrative Code, was transferred to the DMS Rules, Chapter 60GG-2, Florida Administrative Code. AST Rules, Chapter 74-2 was in effect during our audit period (July 2018 through March 2019).

[5] AST Rule 74-2.003(5)(d), Florida Administrative Code.

[6] Agency Policy PD 14-006, *Agency Information Security Program Policy*.

[7] Agency Policy PD 14-001, *Agency Information Security Incident and Breach Response Policy*.

We also found that the *Agency Information Security Program*, *Information Security Incident and Breach Response*, and the *Computer Security Incident Response Team* policies had not been updated since October 22, 2012, to reflect current Agency processes and AST rule requirements. The lack of updated security policies may have contributed to the deficiencies discussed in Findings 2 and 3.

A comprehensive information security program that includes up-to-date information security policies, procedures, standards, and guidelines; an information security awareness program; and an information security risk management process that includes a CSIRT helps provide security for the operations and assets of the Agency. Additionally, up-to-date policies and procedures that address security awareness training, categorizing security incidents, incident escalation, data backups, and patch management further reduce the risk that Agency data and IT resources may be compromised.

Recommendation: We recommend that Agency management ensure that the Agency information security program includes all relevant security policies and procedures to appropriately protect the information and information systems that support the operations and assets of the Agency.

Finding 2: Security Awareness Training

AST rules[8] require State agencies to provide their employees cybersecurity awareness education and training to ensure they perform their cybersecurity-related duties and responsibilities consistent with agency policies and procedures within 30 days after hire and annually thereafter.

As part of our audit procedures, we reviewed the Agency's employee security awareness training records and determined that security awareness training for newly hired employees was not always completed within 30 days of employment and annually thereafter, contrary to AST rules. Specifically, we examined the security awareness training records as of March 29, 2019, and found that:

- For 12 of the 38 employees tested who were hired during the period July 1, 2018, through December 27, 2018, security awareness training was not completed within 30 days of the employees' hire dates. For 9 of the 12 employees, the security awareness training was not completed until 3 to 158 days after the 30-day period had elapsed. For the other 3 employees, the security awareness training had not been completed as of March 29, 2019, and, at that date, was 75 to 159 days late.
- 19 of the 40 employees tested who were hired prior to July 1, 2018, had not received annual security awareness training. Agency records did not evidence that 1 of the employees had completed security awareness training since the employee was hired in 2016. Our examination of the security awareness training records for the other 18 employees found that the dates of the most recently completed security awareness training ranged from August 3, 2015, to August 2, 2017.

Timely security awareness training and reinforcement of security practices through such training help to protect the confidentiality, integrity, and availability of Agency data.

Recommendation: We recommend that Agency management ensure security awareness training is timely completed in accordance with AST rules.

[8] AST Rule 74-2.003(2) and (3)(b) and (c), Florida Administrative Code.

Finding 3: Computer Security Incident Response

AST rules[9] require agencies to establish and maintain response processes and procedures and validate execution capability to ensure timely agency response for detected cybersecurity incidents. Agencies are also required to establish a CSIRT to respond to cybersecurity incidents. CSIRT member responsibilities include, but are not limited to, convening at least quarterly to review, at a minimum, established processes and escalation protocols; and receiving incident response training annually.

We reviewed Agency records related to the eight cybersecurity incidents the Agency reported to the CSIRT during the period January 1, 2018, through December 28, 2018, to determine whether the incidents were sufficiently documented, including an assessment of the risk and severity of the incident; necessary corrective actions were taken; and incidents were reported as required to the AST. For four of the eight cybersecurity incidents, Agency records did not evidence an assessment of the risk and the severity of the incident and the necessary corrective action was not documented for one of the four incidents. Our examination also found that the Agency's security incident response form, which included a place to record the severity of security incidents, was not completed for the four incidents noted above.

Our audit procedures also disclosed that the Agency CSIRT did not convene at least quarterly in 2018. While Agency management indicated that quarterly meetings were held for two of the four quarters in 2018, meeting notes were not maintained to evidence the quarterly CSIRT meetings held. Agency management also indicated that a CSIRT quarterly meeting was not held for the first quarter because the CSIRT members were busy responding to an incident and the meeting for the fourth quarter was not held because Agency staff were busy implementing a new system. Additionally, annual CSIRT member training on cybersecurity threats, trends, and evolving practices was not provided during 2018. In response to our audit inquiry, Agency management stated that discussions on various cybersecurity topics took place during CSIRT meetings; however, formal cybersecurity incident response training was not provided during the period of January 1, 2016, through May 2, 2019.

Absent sufficient investigation and documentation of computer security incidents, including an assessment of the risks and identification of the severity of the incidents, the risk is increased that cybersecurity incidents will not be timely and appropriately detected, responded to, and corrected. CSIRT meetings that review established processes and escalation protocols and annual CSIRT member training promote prompt and appropriate responses to cybersecurity incidents.

Recommendation: We recommend that Agency management ensure that cybersecurity incidents are sufficiently assessed and documented, CSIRT meetings are conducted at least quarterly, and CSIRT members receive annual training as required by AST rules.

Finding 4: Timely Disabled Network Access Privileges

Effective management of IT access privileges includes the timely disablement of IT access privileges when an employee separates from Agency employment or when the use of an account is no longer

[9] AST Rule 74-2.005(1), Florida Administrative Code.

necessary. Prompt action is necessary to ensure that the access privileges are not misused by former employees or others to compromise data or IT resources.

Our review of Agency records for 6 of the 64 former employees who worked in two budget entities within the Agency requiring network access privileges and separated from Agency employment during the period July 1, 2018, through December 27, 2018, found that the network user accounts of 2 former employees remained enabled as of January 24, 2019, 70 and 85 days, respectively, after the employees' separation from Agency employment. While the network user accounts were disabled for the other 4 former employees, Agency records did not evidence the disabled dates; therefore, Agency management could not demonstrate that the network user accounts of the 4 former employees were timely disabled.

Through additional audit procedures, we found another 13 network user accounts assigned to former employees in two other budget entities. Our evaluation of the 13 network user accounts disclosed that, as of January 24, 2019, 1 network user account assigned to a former employee remained enabled 188 days after the employee's separation date. While the other 12 network user accounts were disabled as of January 24, 2019, Agency records did not evidence the disabled dates; therefore, the Agency was unable to demonstrate that the network user accounts were timely disabled.

Timely disabling network user accounts upon an employee's separation from Agency employment reduces the risk that the network access privileges may be misused by the former employee or others.

Recommendation: To minimize the risk of compromise to Agency data and IT resources, we recommend that Agency management ensure that network access privileges are timely disabled upon an employee's separation from Agency employment. In addition, the Agency should retain records evidencing the dates accounts are disabled.

Finding 5: Periodic Access Review

AST[10] rules require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. An effective periodic review consists of identifying the current access privileges of all system users and evaluating the assigned access privileges to ensure that they align with the users' job responsibilities.

Our audit procedures disclosed that, while the Agency had policies that required periodic reviews of user access privileges, the processes and procedures for implementing the periodic review policies need improvement. Specifically, we found that:

- The *Criminal Justice Information Services* (*CJIS*) *Security Compliance Policy*[11] requires the Agency to validate Agency user accounts (CJIS and non-CJIS users) and access privileges annually. Our audit procedures disclosed that, while the Agency validated access to CJIS data on an ad hoc basis, including network user accounts, the Agency did not at least annually use a system-generated list of all network user accounts (CJIS and non-CJIS) to evaluate whether each user's network access remained appropriate.

[10] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[11] Agency Policy and Operating Procedure 6-0024, *Policy and Procedures for CJIS Security Compliance* (*CJIS Security Compliance Policy*).

- The Agency's *Information Technology Workers Policy*[12] requires the Information Security Access Control Office to periodically review administrative credentials (user accounts) to verify that only authorized individuals have administrative (privileged) access to Agency network resources and data. However, in response to our audit inquiry, Agency management indicated that they only reviewed the administrative credentials of network users in an ad hoc manner without a documented process or procedures and that evidence of review was not maintained. The review was also limited to privileged network user accounts and did not include administrative credentials for other high-risk network resources.

Without a comprehensive periodic access review, management's assurance that the user access privileges assigned are authorized and remain appropriate is limited.

Recommendation: We recommend that Agency management develop documented procedures to facilitate effective periodic reviews of all user accounts, including all privileged administrative accounts.

Finding 6: Security Controls – Logical Access, User Authentication, Configuration Management, Logging and Monitoring, and Vulnerability Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Agency data and other Agency IT resources. However, we have notified appropriate Agency management of the specific issues.

Without appropriate security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management, the risk is increased that the confidentiality, integrity, and availability of Agency data and IT resources may be compromised.

Recommendation: We recommend that Agency management improve certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management to ensure the confidentiality, integrity, and availability of Agency data and other IT resources.

PRIOR AUDIT FOLLOW-UP

The Agency had taken corrective actions for Finding 5 included in our report No. 2016-071.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

[12] Agency Policy 6-0018, *Policy Governing the Acceptable Practices for Information Technology Workers* (*Information Technology Workers Policy*).

We conducted this IT operational audit from October 2018 through May 2019 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT general controls applicable to Agency operations during the period July 2018 through March 2019 and selected actions prior and subsequent thereto. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, a deficiency disclosed in our report No. 2016-071 applicable to the scope of this audit.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Agency personnel and reviewed related documentation to obtain an understanding of:
  - Security logging and monitoring controls for the network and high-risk network devices.
  - Logical access and authentication controls for administrative network users.
  - Configuration management processes for high-risk network devices, including patches, upgrades, and other configuration changes.
  - Security awareness training, incidence response, vulnerability management, and background screening processes.
- Evaluated logical access controls for administrative access to high-risk network devices, servers, and the Agency's network. Specifically, we evaluated the appropriateness of:
  - Administrative accounts as of January 7, 2019, for the 10 high-risk network devices.
  - Local administrative accounts as of March 7, 2019, for 10 of the 56 servers in production as of February 25, 2019.
  - The 19 unique privileged network user accounts and the 11 privileged network service accounts as of January 3, 2019, with membership in the *Enterprise Admins*, *Schema Admins*, and *Domain Admins* security groups, and as of February 28, 2019, in the *Administrators* security group.
- Evaluated the effectiveness of logical access controls for periodic access reviews of network user accounts and high-risk network device administrative accounts and the timely disabling of network user accounts. Specifically, we:
  - Evaluated Agency procedures for periodic reviews of users assigned privileged and non-privileged network user accounts and high-risk network device administrative accounts to assess the adequacy of periodic review procedures.
  - Compared the list of Agency employees who separated from Agency employment during the period July 1, 2018, through December 27, 2018, and worked in Agency budget entities 67100100 and 67100200, to the list of network user accounts as of January 24, 2019, to determine whether any former employees retained their network user accounts beyond their separation dates.
  - Conducted additional audit procedures as of January 24, 2019, to determine whether selected former Agency employees who worked in Agency budget entities 67100400 and 67100500 and separated from Agency employment during the period July 1, 2018, through December 27, 2018, retained their active network user accounts beyond their separation dates.
- Evaluated the adequacy of logging and monitoring controls for network and high-risk network device administration and activity.
- Evaluated the adequacy of network identification and authentication controls including policies and procedures and authentication settings for network access and high-risk network device administration.
- Evaluated configuration management controls for high-risk network devices. Specifically, we:
  - Evaluated the adequacy of Agency policies and procedures regarding configuration management.
  - Evaluated the 10 Agency-managed high-risk network devices as of May 2, 2019, to determine whether the firmware was up to date.

- Evaluated data backup policies, procedures, and processes for Agency-managed servers. Specifically, we:
  - Evaluated the adequacy of Agency policies and procedures regarding data backup processes.
  - Evaluated the 28 active Agency-managed servers as of January 23, 2019, to determine whether backup processes were timely and successful.
- Evaluated incident response activities (i.e., CSIRT membership, meeting, training, and incident reporting policies, procedures, and processes).
- Evaluated the entity-wide security awareness training program, including security awareness policies and procedures, new hire training, and annual training for all staff. Specifically, we examined the training records for:
  - 38 of the 325 employees and the 1 IT contractor hired by the Agency during the period July 1, 2018, to December 27, 2018, to determine whether security awareness training was completed within 30 days of their respective hire dates.
  - 40 of the 2,598 active employees as of March 11, 2019, and the 12 active IT contractors as of February 28, 2019, with a hire date prior to July 1, 2018, to determine whether the employees and IT contractors had completed annual security awareness training within the past year.
- Evaluated the vulnerability management controls to determine whether the vulnerability management plan included vulnerability management policies and procedures, and processes for vulnerability scanning, timely analysis, and remediation.
- Evaluated background screening controls for staff (employees and IT contractors), including background screening policies, procedures, and processes. Specifically, we examined the background screening records for 38 of the 325 employees hired during the period July 1, 2018, through December 27, 2018, and all 13 IT contractors employed as of February 22, 2019, to determine whether level 2 background screenings were performed timely.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

agency for persons with disabilities
State of Florida

Ron DeSantis
Governor

Barbara Palmer
Director

State Office
4030 Esplanade Way
Suite 380
Tallahassee
Florida
32399-0950

(850) 488-4257
Fax:
(850) 922-6456

Toll Free:
(866) APD-CARES
(866-273-2273)

August 22, 2019

Sherrill F. Norman, CPA
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Re: Preliminary and Tentative Audit Findings – Agency for Persons with Disabilities, Information Technology General Controls

Dear Ms. Norman:

I appreciate this opportunity to respond to the preliminary and tentative audit findings and recommendations concerning your information technology operational audit of the *Agency for Persons with Disabilities, Information Technology General Controls*. Our response is enclosed as required by section 11.45(4)(d), Florida Statutes.

I appreciate the effort of you and your staff in assisting to improve our operations. If you have any questions or need additional information, please contact Shawn McCormick, Director of Audit at (850) 414-8774.

Sincerely,

for

Barbara Palmer
Director

BP/sm
Enclosure

AGENCY FOR PERSONS WITH DISABILITIES, INFORMATION TECHNOLOGY GENERAL CONTROLS

Finding No. 1: Information Security Program

Finding: The Agency's *Information Security Program Policy* did not encompass or reference significant aspects of a comprehensive information security program.

Recommendation: We recommend that Agency management ensure that the Agency information security program includes all relevant security policies and procedures to appropriately protect the information and information systems that support the operations and assets of the Agency.

Agency Response: The Agency for Persons with Disabilities (Agency) concurs with this finding.

The Agency will write the recommended security awareness training policy/procedure.

The Agency will formally add its current incident handling protocol, which includes requirements for categorizing security incidents, to its *Information Security Incident and Breach Response Policy*.

The Agency will write the recommended Agency-managed server data backup policy/procedure.

The Agency will write the recommended firmware patches policy/procedure.

Finding No. 2: Security Awareness Training

Finding: Security awareness training for Agency employees was not always completed timely.

Recommendation: We recommend that Agency management ensure security awareness training is timely completed in accordance with AST rules.

Agency Response: The Agency concurs with this finding.

The Agency is analyzing the causes of this problem and will develop strategies to address it.

Finding No. 3: Computer Security Incident Response

Finding: Agency computer security incident response processes need improvement.

Recommendation: We recommend that Agency management ensure that cybersecurity incidents are sufficiently assessed and documented, CSIRT meetings are conducted at least quarterly, and CSIRT members receive annual training as required by AST rules.

Agency Response: The Agency concurs with this finding.

The Agency will exercise more care to ensure Incident documentation is complete.
The Agency will ensure all regularly scheduled Quarterly CSIRT meetings occur.
The Agency will deliver training to the CSIRT more formally.

Finding No. 4: Timely Disabled Network Access Privileges

Finding: The Agency did not timely disable the network access privileges for some former employees.

Recommendation: To minimize the risk of compromise to Agency data and IT resources, we recommend that Agency management ensure that network access privileges are timely disabled upon an employee's separation from Agency employment. In addition, the Agency should retain records evidencing the dates accounts are disabled.

Agency Response: The Agency concurs with this finding.

The Agency is already taking steps to address this finding by ensuring closer coordination between Information Security and Human Resources and will continue in these efforts.

Finding No. 5: Periodic Access Review

Finding: Agency policies and procedures for periodic reviews of access privileges need improvement.

Recommendation: We recommend that Agency management develop documented procedures to facilitate effective periodic reviews of all user accounts, including all privileged administrative accounts.

Agency Response: The Agency concurs with this finding.

The Agency is developing procedures to address this finding.

Finding No. 6: Security Controls - Logical Access, User Authentication, Configuration Management, Logging and Monitoring, and Vulnerability Management

Finding: Certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management need improvement.

Recommendation: We recommend that Agency management improve certain security controls related to logical access, user authentication, configuration management, logging and monitoring, and vulnerability management to ensure the confidentiality, integrity, and availability of Agency data and other IT resources.

Agency Response: The Agency concurs with this finding.

The Agency will take actions to improve certain security controls.