FLORIDA DEPARTMENT OF JUVENILE JUSTICE

INTEROFFICE MEMORANDUM

DATE: June 25, 2018

TO: Christina K. Daly, Secretary
Eric Miller, CIG, Executive Office of the Governor

FROM: Robert A. Munson, Inspector General

SUBJECT: Final Report – Audit No. A-1718DJJ-004, *Audit of Network Security*

Please find enclosed our final report for the *Audit of Network Security*. The Bureau of Internal Audit will conduct a follow-up review in six months to determine the status of corrective actions taken to address the reported findings.

We would like to thank the Bureau of Information Technology for the assistance extended to our staff during the audit process. Please feel free to contact Michael Yu, Audit Director, at 850-717-2468 if you have any questions.

RM/my/kn

Attachment

Cc: Timothy Niermann, Deputy Secretary
Fred Schuknecht, Chief of Staff
Vickie Harris, Director of Administration
Dennis Hollingsworth, Chief Information Officer
Sherrill F. Norman, Auditor General
Kathy DuBose, Director, Legislative Auditing Committee

Audit of Network Security
Audit No. A-1718DJJ-004
June 25, 2018

By

The Office of the Inspector General
Bureau of Internal Audit

Robert A. Munson
Inspector General

Michael Yu, CIA, CIG
Director of Auditing

Kelly Neel
Auditor-in-Charge

Office of Inspector General
Bureau of Internal Audit
Audit of Network Security
Audit No. A-1718DJJ-004

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Juvenile Justice (Department), Office of the Inspector General, Bureau of Internal Audit has performed an Audit of Network Security. The overall objectives of this audit were to provide management with an independent assessment relating to the effectiveness of the network security and the implementation of the Bureau of Information Technology (IT) network security policies; provide management with an evaluation of the IT network function's preparedness in the event of a disaster; and identify issues that affect the security of the network. The audit focused on network security, including associated policies, standards and procedures, as well as the effectiveness of the security implementation from July 1, 2016 through June 30, 2017, and related activities through the end of fieldwork.

The audit disclosed that, in general, the Department had IT related policies and procedures in place that complied with Florida Statutes and Florida Administrative Codes (F.A.C.).

However, we noted the following areas for improvement:

- Network security policy, procedures, and diagram were not available,
- Network server room access was not limited to authorized users and procedures regarding access to the server room were not developed or implemented,
- External penetration testing and internal security self-assessments have not been implemented, and
- The review and audit of activities of those with administrative privileges was not documented.

We recommended the Department implement processes to enhance oversight of network security.

The Bureau of Information Technology concurred with the findings and recommendations.

Audit of Network Security

INTRODUCTION

The Office of the Inspector General, Bureau of Internal Audit, conducted an audit of Network Security from July 1, 2016 through June 30, 2017, and related activities through the end of fieldwork. This audit was initiated based on our Fiscal Year 2017-2018 Audit Plan and conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors.

Background

The Bureau of Information Technology (IT), located within the Department's Office of Administrative Services, works in conjunction with the Agency for State Technology (AST) to establish Network Security for the Department.

The AST was established in 2014 by the Florida Legislature, to develop and publish information technology policy for the management of the State's information technology resources, oversee the State's essential technology projects, and manage the State Data Center (SDC). The AST receives funding from the legislature to provide network infrastructure for state agencies, as well as operate and maintain the SDC.

As part of the network security services to the Department, AST provides monitoring for malware, and suspicious traffic that could infect or breach the DJJ network. Malware alerts go to the AST first; then the AST will notify the Department of any alerts. The AST also notifies/alerts the DJJ network of unusual network traffic. Additionally, the AST is responsible for vulnerability scanning and continuous monitoring of 80 DJJ servers located at the SDC.

IT is responsible for IT planning and resource management including, but not limited to, technology planning; server administration and support services; internet security and firewall management; network telecommunication services; video teleconferencing services; applications development, support, and maintenance; data administration, data line installation, management, and monitoring at all DJJ sites.

The IT Network & Infrastructure unit is responsible for network data line installation and management, implementation of network security measures, and monitoring to identify, detect, and block malicious activity. The unit is also responsible for maintaining the hardware for production, developing and testing servers, and managing Active Directory, internet, and email security. The Department's Computer Security Incident Response Team (C-SIRT) is responsible for reporting, responding, mitigating, and tracking computer security incidents, which occur within the agency and applicable service providers.

Objectives, Scope, and Methodology

The overall objectives of this audit were to provide management with an independent assessment relating to the effectiveness of the network security and the implementation of IT network security policies; provide management with an evaluation of the IT network function's preparedness in the event of a disaster; and identify issues that affect the security of the network. The audit focused on network security, including associated policies, standards and procedures, as well as the effectiveness of the security implementation from July 1, 2016 through June 30, 2017, and related activities through the end of fieldwork.

To achieve the audit objectives, we:

- reviewed applicable statutes and rules;
- reviewed department policies and procedures;
- interviewed IT staff;
- reviewed network security design
    - Security risk analysis
    - Security policy
    - Trust zones
    - Hardened systems
- reviewed network security components
    - Routers
    - Switches
    - Firewalls
    - Remote access – VPNs
    - Wireless networking
    - Intrusion detection
    - Network security assessments

RESULTS OF AUDIT

Network perimeter security is a process to ensure the protection of the Department's data, assets and information that are stored on computer equipment residing on the network and the information flowing through the network.

Network perimeter security is built on the idea that layers of security components, when combined, provide the necessary protection from unauthorized access to the network. This process includes:

- Security policy built on good practices,
- Authorization and access controls addressed by identity management,

- External perimeter control using firewalls to protect the internal network from external intrusion;
- Virtual private networks (VPNs) to allow authorized traffic through the firewall, using encryption techniques,
- Intrusion detection tools to identify suspect network activity and issue alerts,
- Penetration testing to ensure that firewalls are securely configured,
- Internal security assessments to evaluate policy and procedures,
- Risk management to evaluate and identify networks and resources requiring enhanced security, and
- Internal network segmentation, limiting access of data in certain locations to authorized users and restricting that area from others within the enterprise.

The Department's network is the primary communications channel since applications function through the network; financial transactions are stored and processed; e-mail containing confidential information is exchanged; analysis, business strategy, and presentations, are stored and exchanged; and personal identification information may be stored and transmitted.

This audit disclosed that in general, the Department had policies and procedures in place regarding IT security that complied with Florida Statutes and Florida Administrative Codes and preparedness in the event of a disaster. However, we noted areas for improvement.

Details of Findings and Recommendations

Finding 1: Network security policy, procedures, and diagram were not available.

F.A.C. 74-2.003 (5)(a)1 and 2 state each agency shall ensure that security policies, processes and procedures are maintained and used to manage protection of information systems and assets. Such policies, processes and procedures shall include a current baseline configuration of information systems. Baselines shall specify standard hardware and secure standard configurations and include documented firewall and router configuration standards, and include a current network diagram.

While there are policies and procedures department wide relating to overall network security, there is not a documented network security policy specific to the application and operating system and detailed enough to enable a knowledgeable user to perform the procedure or configure the system or application. Also, a department-wide inventory of network assets and a diagram of all network devices and how they are connected was not available. The inventory of network assets and network diagram would help with network size estimation, network capacity planning, network cost estimation and physical network administration.

When discussed, IT management advised that they have not had the resources to comply fully with this rule. However, they provided that the Bureau of General Services launched a department wide inventory process in December of 2017. This process included IT assets, including network related hardware. The process tracks assets by utilizing handheld scanners that document property identification information, including Department property numbers and individual asset serial numbers. This new process allows the Department to track and protect IT assets.

We recommend developing and implementing a network security policy to identify the good practices of an accepted network standard and establish a clear network security strategy. The strategy should specify the types of controls, such as demilitarized zones (DMZs), trust zones, hardened operating systems, least privilege and separation of duties, that should be implemented and supported by documented detailed security procedures and standards. We also recommend the Bureau of Information Technology creating an enterprise-wide information asset inventory that specifies information owner and information criticality.

Additionally, we recommend the Department develop a network diagram that may be useful when technicians are trying to track down problems within a network. Often, these issues can be more easily traced if the technicians understand how all the different devices in a network are connected to each other. Network diagrams are also useful for network engineers and designers, as it helps them to compile detailed network documentation.

Finding 2: Network server room access was not limited to authorized users and procedures regarding access to the server room were not developed or implemented.

F.A.C. 74-2.003 (1)(b)2-5 state that each agency shall implement procedures to manage physical access to IT equipment, identify physical controls that are appropriate, specify physical access to equipment that is restricted to authorized personnel, and detail visitor access protocols, including logging procedures and requiring that visitors be supervised.

During the audit fieldwork, security control deficiencies were identified related to server room I.D. card access. Specifically, the Bureau of General Services was not accurately assigning I.D. card access when activating Department employee I.D. cards. Additionally, IT was not verifying that server room access was only available for authorized users.

During our review of employee I.D. card access to the Knight Building network server room, it was discovered that 96 Department I.D. cards permitted access to the server room, as follows:

- 20 Koger Center employees,

- 5 Alarm Company employees,
- 7 Bureau of General Services employees,
- 17 Bureau of Information Technology employees,
- 2 Office of Inspector General employees,
- 1 Bureau of Human Resources employee, and
- 44 General Access employees (consisting of employees within the Office of General Counsel, Staff Development & Training, Office of the Secretary, Administration, Detention, Prevention, Probation, Residential, Communications, and Research & Data Integrity)

Failure to establish and implement appropriate procedures governing access to the network server room could result in loss or damage of physical assets. Moreover, an unintentional or intentional outage could result in significant productivity loss.

During audit fieldwork, auditors notified IT of this issue. IT and General Services addressed server room access immediately and reduced the number of I.D. cards with access to 15, consisting of:

- 1 Koger Center employee,
- 1 Alarm Company employee,
- 3 Bureau of General Services employees,
- 9 Bureau of Information Technology employees, and
- 1 General Access employee.

Additionally, General Services is in the process of updating their Employee I.D. Card Access Request Form.

We recommend the Department develop and implement a procedure governing server room access, including an annual review of the Server Room Access List by IT management and consider adding video surveillance as an extra layer of protection.

Finding 3: External penetration testing and internal security self-assessments have not been implemented.

F.A.C. 74-2.002 (4)(b)1 and 3 state that each agency shall identify and document asset vulnerabilities, business processes and protection requirements; establish procedures to analyze systems and applications to ensure security controls are effective and appropriate; and identify and document internal and external threats.

During the audit review, it was determined that IT has not implemented external penetration testing or internal security self-assessments. When discussed, management advised that IT does not have the tools for self-assessments. However, management

indicated they would be working with the Chief Information Security Officer at the Agency for State Technology to formulate a plan for penetration testing.

The main objective for a network penetration test is to identify available vulnerabilities in networks, systems, hosts and network devices before hackers can discover and exploit them. Network penetration testing can reveal actual opportunities that hackers might exploit to compromise systems and networks in such a way that allows for unauthorized access to sensitive data or even take-over systems for malicious purposes.

The effective implementation of an internal network self-assessment that reviews the configurations, policies and utilization of network appliances can increase the value of the Department's information security program. Self-assessments are performed to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, management and other personnel to collaborate and view the entire organization from an attacker's perspective. Without penetration testing and self-assessments, the department could unknowingly be vulnerable to exploitation.

We recommend the Department implement regularly scheduled penetration testing and self-assessments.

Finding 4: The review and audit of activities of those with administrative privileges is not being documented.

Department Policy DJJ1235 Utilization of Information Technology Access Privileges and Resources indicates that the use and activities of those with elevated administrative privileges shall be reviewed periodically and audited by the CIO (or designee) to ensure said privileges are used in accordance with assigned duties and responsibilities.

During our review, auditors determined the review and audit process was rather informal and not documented. Therefore, confirming privileges were in accordance with assigned duties and responsibilities could not be assessed by management and the review and audit process could not be verified.

Unmanaged administrator rights could lead to incidents of employees downloading and installing unauthorized software without understanding the potential risks associated with their actions, such as malware exploits and targeted cyberattacks.

We recommend the Department retain documentation of the periodic reviews and audits conducted by the CIO (or designee) of the activities of all staff with administrative privileges.

APPENDIX

MANAGEMENT RESPONSE

FLORIDA DEPARTMENT OF JUVENILE JUSTICE

INTEROFFICE MEMORANDUM

DATE: June 25, 2018

TO: Robert Munson, Inspector General

FROM: Dennis Hollingsworth, Chief Information Officer

SUBJECT: Audit of Network Security Response, Audit No. A-1718DJJ-004

Please find below the response to the preliminary findings and recommendations.

Finding 1: Network security policy, procedures, and diagram were not available.

We concur. To ensure the agency remains in compliance with F.A.C. 74-2.003 (5)(a) 1 and 2, IT management will work to develop and implement a network policy that establishes clear network security strategies for demilitarized zones, trust zones, hardened operating systems, least privilege network use and separation of duties. In addition, IT will develop a comprehensive network diagram that includes ingress and egress points, network traffic flows and connections related to internal DJJ network equipment up to the point where the connection becomes an AST network component. We anticipate completion of these changes by November 2018.

Finding 2: Network server room access was not limited to authorized users; and procedures regarding access to the server room were not developed or implemented.

We concur. It was realized through the course of this audit that access to the Knight Building server room was not limited to authorized users only. Upon being notified of this deficiency, IT management worked with the Bureau of General Services to immediately address this issue. As a result, the list of personnel with access to the Knight building IT Server Room was reduced from 96 to 15 personnel the day after the issue was identified. To prevent future unauthorized access to the Knight Building IT Server Room, the Bureau of General Services is currently finalizing modifications to the Employee I.D. Card Access request form which will require any access to the IT Server Room to be approved

in advance by the DJJ Chief Information Officer. The associated policies and procedures will be updated to reflect these process changes and will also include additional language requiring IT management to conduct a periodic review of IT Server Room access. We anticipate completion of these changes by July 2018.

Finding 3: External penetration testing and internal security self-assessments have not been implemented.

We concur. To address these issues, IT will work internally as well as with the Agency for State Technology (AST) to develop planned network assessments. This includes, but is not limited to penetration testing and self-assessments of network security as allowed by legislation and AST. Based on past communication from AST, we will soon be able to utilize tools planning to be acquired by AST for this purpose. Afterwards, we will be able to gauge the remaining security needs of the agency and plan purchases accordingly. The timeframe to obtain access to the tools provided by AST, develop the associated processes, and fully implement these processes will be dependent upon AST providing the above-mentioned tools. We anticipate completion of these changes by November 2018.

Finding 4: The review and audit of activities of those with administrative privileges is not being documented.

We concur. The IT department will begin periodic reviews and audits of staff whose DJJ network accounts include administrative privileges. The CIO (or designee) will document the review as a matter of compliance with DJJ Policy1235. We anticipate implementation of these changes by July 2018.