OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Education

Information Technology Security Controls Audit

As of March 2013

August 29, 2013 **Report 13-20**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us
Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

August 29, 2013

Senator Roger Reinert, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Dr. Brenda Cassellius, Commissioner
Department of Education

Matthew Porett, Department of Education's Chief Information Officer
Office of MN.IT Services

This report presents the results of our audit to determine whether the Department of Education had adequate information technology controls, as of March 2013, to protect data from unauthorized access or modification and to ensure that changes made to the department's significant applications and supporting infrastructure were authorized. We emphasize that this has not been a comprehensive audit of the Department of Education.

We discussed the results of the audit with the department's staff at an exit conference on August 20, 2013. This audit was conducted by Carolyn Engstrom, CPA, CISA (Audit Manager) David Westlund, CPA, CISA (Auditor-in-Charge), and auditor Thom Derus.

We received the full cooperation of the department's staff while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Phone: 651-296-4708 • Fax: 651-296-4712
E-mail: legislative.auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Report Summary

Conclusion

The Department of Education did not have adequate internal controls to ensure that it appropriately limited access to its data and protected the hardware and software that support its significant computer applications.[1]

Findings

- The Department of Education's significant computer applications did not have comprehensive security plans. (Finding 1, page 7)
- The security controls for one of the Department of Education's most important operating systems were not adequate to protect not public information. (Finding 2, page 8)
- The expected security settings were not documented for the Department of Education's significant computer applications. Also, changes to the applications could occur without complying with the change management plan. (Finding 3, page 9)
- Servers supporting the Department of Education's significant applications were not adequately monitored for vulnerabilities. (Finding 4, page 10)
- The Department of Education lacked documented processes to authorize and review access to its significant applications' supporting hardware and software by staff from the Office of MN.IT Services. (Finding 5, page 12)

Audit Objective and Scope

The audit objective was to determine whether the Department of Education had adequate information technology controls, as of March 2013, to protect data from unauthorized access or modification and to ensure that changes made to the department's significant computer applications and supporting hardware and software were authorized.

[1] The Department of Education's significant applications included the Integrated Department of Education Aid System (IDEAS) which processed state school aid payments; the State Educational Record View and Submission System (SERVS) which processed federal school aid payments; and versions one and two of the Cyber-linked Interactive Child Nutrition System (CLiCS1 and CLiCS2), which processed federal food and nutrition program payments.

Department of Education

Information Technology Security Controls

Overview

The Department of Education uses over a hundred applications to support its diverse responsibilities, such as teacher licensing, school lunch programs, special education oversight, and distributions of school aids. Two applications, Integrated Department of Education Aid System (IDEAS) and State Educational Record View and Submission System (SERVS), process federal and state school aid payments. These payments are significant to the state's financial statements; in fiscal year 2012, IDEAS payments totaled about $6.6 billion and SERVS payments totaled about $700 million. Two other applications, Cyber-linked Interactive Child Nutrition System, versions one and two (CliCS1 and CliCS2), process transactions for federal food and nutrition programs.

The Department of Education obtains support for its information technology through a service level agreement with the Office of MN.IT Services (MN.IT).[2] As of March 2013, 60 MN.IT staff assigned to the department managed over 1,000 department computers, servers, mobile devices, and printers required by its applications and employees.[3] Department-based MN.IT staff also provided the department with application development services, system security services, and help desk assistance.

The service level agreement acknowledges the need for communication, coordination, and cooperation between the Department of Education and the Office of MN.IT Services as they share the responsibility for the security of the department's computer systems and the protection of data in the related databases. The service level agreement includes the following goals:

- Define services in terms that make sense to the agencies.

- Identify the processes by which agency management can, with help from MN.IT Services, make business decisions and set priorities for information technology.

[2] *Minnesota Laws* 2013, Chapter 134, Section 30, changed the name of the Office of Enterprise Technology to the Office of MN.IT Services.

[3] Department-based MN.IT staff work on-site within executive branch agencies, such as the Department of Education, to support their specific information technology needs. In 2011, when the state consolidated its information technology services, most of the state's information technology employees became department-based MN.IT staff, reporting through the department-based MN.IT chief information officer to the state's chief information officer. Many of the department-based MN.IT staff continued to perform the same duties as they had before the consolidation.

- Clarify roles so that agencies know what services MN.IT delivers.

- Create performance indicators so that agency management knows that the documented expectations are being met.

The Department of Education is responsible for assessing risks related to data protection and approving the appropriate controls to mitigate the risks. Section 7 of the service level agreement further defines the roles of the department, department-based MN.IT staff, and the Office of MN.IT Service's Enterprise Security Office regarding the state's enterprise security program. The Department of Education must understand and establish an acceptable level of risk and ensure that the minimum state security policy requirements can be met in their department. Department-based MN.IT staff are responsible for complying with enterprise security program policies and standards, consulting with department leadership to develop standards not yet addressed by the Enterprise Security Office, and ensuring that mitigating controls are in place to reduce risk to the department's acceptable level of risk. Through cooperation, the department and its department-based MN.IT staff determine what the appropriate level of risk is for the department's data.

Objective, Scope, and Methodology

The audit objective was to answer the following questions:

- Did the Department of Education have adequate internal controls to ensure that data contained in its significant applications (IDEAS, SERVS, CLiCS1, and CLiCS2) could not be modified outside of application processing without proper approval?

- Did the Department of Education have adequate internal controls to ensure that changes made to its significant applications and their supporting hardware and software were authorized?

- Did the Department of Education have adequate information technology security controls to protect data from unauthorized access?

To answer these questions, we interviewed management of the Department of Education and department-based MN.IT staff. We reviewed relevant documentation and used a variety of computer-assisted auditing tools to analyze the system's security controls. We assessed the effectiveness of the following internal controls:

- Access controls – Were password policies and other authentication mechanisms effective to appropriately restrict users' access? Were users given only the access they needed to perform their job duties? Were

certain incompatible duties segregated? If not, was appropriate monitoring in place to ensure that transactions were accurate and authorized?

- Change management controls – Were management expectations for system settings documented? Were changes to the system requested, tested, and authorized? Were changes to the system monitored to detect unauthorized changes?

- Vulnerability management – Were vulnerabilities identified, analyzed, and mitigated?

We did not test whether people with authorized access through the department's applications used that access to modify or view not public data beyond the needs of their work assignments.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, published by the National Institute of Standards and Technology's Computer Security Division. When available, we also used department and state policies to obtain evaluation criteria. We also used criteria contained in security guidance, published by the Defense Information Systems Agency, and information published by applicable technology vendors to evaluate select controls.

Conclusion

The Department of Education did not have adequate internal controls to ensure that it appropriately limited access to its data and protected the hardware and software that support its significant computer applications.

The following *Findings and Recommendations* section provides further explanation about the department's deficiencies.

Findings and Recommendations

Finding 1

The Department of Education's significant computer applications did not have comprehensive security plans.

The Department of Education's applications, including its significant applications, did not have comprehensive security plans. Although department and department-based MN.IT staff had developed and documented some attributes of a system security plan, some gaps existed.[4] For example, though an overall security categorization of the system was provided, there was limited documentation to support the assessment, such as a formal assessment of the applications' separate requirements of confidentiality, integrity, and availability in order to arrive at the overall security classification.[5]

Further, while applications were noted to contain public, confidential, private, nonpublic, or protected nonpublic data, the department had not documented the specific not public data elements it contained. Although, the department's data practice officer, legal counsel, program owners, and certain information technology staff were able to fairly consistently describe for us the not public data contained in its significant applications, the department had not documented the not public data it possessed, where it resided on its systems, or management's expectations about the internal controls needed to secure it.

Without developing a comprehensive security plan and not assessing its systems' confidentiality, integrity, and availability requirements, management may implement system security internal controls that are ineffective (too weak for data protection needs) or inefficient (too strong or costly for data protection needs). Additionally, by not clearly documenting the data that needs to be protected, the department's efforts to protect data may not be consistently applied by its program staff, data privacy officers, legal counsel, and department-based MN.IT staff.

[4] NIST 800-18 *Guide for Developing Security Plans for Federal Information Systems* describes 16 attributes necessary for creating an information security plan. Some of the attributes are easily inventoried, such as the name of the system, owner, support contacts, and a general description of the system's purpose. Other attributes, such as system categorization, a description of the environment the system operates, laws or regulations affecting the system, and the security controls selected for the system, require further analysis to document.

[5] Confidentiality, integrity, and availability are the terms used in the information technology community to describe the core objective of information security. The objective of confidentiality is that the system's security will ensure that only authorized persons will have access to the information. *Minnesota Statutes* 2012, Chapter 13, Government Data Practices, classifies government data into the following categories: public, confidential, private, nonpublic, or protected nonpublic.

Recommendations

- *The Department of Education, with the assistance of the Office of MN.IT Services, should complete a detailed assessment of the confidentiality, integrity, and availability requirements of applications to conclude on a security categorization.*

- *The Department of Education, with the assistance of the Office of MN.IT Services, should complete application security plans that document expected security controls.*

Finding 2

The security controls for one of the Department of Education's most important operating systems were not adequate to protect not public information.

The operating system that supported one of the Department of Education's significant applications (IDEAS) allowed simple passwords, disallowed enforceable password changes, enabled only system default auditing that was not routinely reviewed, and permitted insecure methods to administer the system. Additionally, three of the operating system's administrator accounts had insecure passwords. While IDEAS did not have significant not public data elements, other applications that resided on the operating system did maintain not public data about students and teachers.

This occurred, at least partially, because expected security controls had not been documented, as identified in Finding 1. Department-based MN.IT staff told us that there are plans to retire this operating system in the next two years, and the cost of implementing additional security controls must be evaluated against the remaining useful life of the operating system. Department-based MN.IT staff purchased tools to assist with improved auditing and monitoring; but, by March 2013, the tools had not been implemented.

Recommendation

- *The Department of Education, with the assistance of the Office of MN.IT Services, should design and implement security controls to adequately protect financial and not public data stored on the operating system.*

Finding 3

The expected security settings were not documented for the Department of Education's significant computer applications. Also, changes to the applications could occur without complying with the change management plan.

The operating systems and databases supporting the Department of Education's significant applications did not have documented standards for their security settings, referred to as configuration baselines. A configuration baseline documents the expected security settings management has established after evaluating the risks posed by the available configuration options.

Department-based MN.IT staff defined a process to record changes to settings in the operating systems, databases, firewalls, and switches supporting the Department of Education's significant applications but did not document it. Additionally, the process did not address the extent of testing or approval required for the system changes. The method of recording the changes did not facilitate the creation of a list of expected changes in order to determine if the changes had been made as authorized.

Department-based MN.IT staff had not implemented controls necessary to detect unauthorized or unlogged changes to the supporting operating systems and databases. Examples of controls designed to detect unauthorized changes would be comparing the system's current configuration to the documented configuration baseline, or enabling auditing of changes in the system and tracing those changes back to the authorization. The state's Enterprise Security Configuration Management Standard requires establishment of internal controls to create, modify, maintain and monitor configuration baselines.[6]

Additionally, for the applications reviewed, department-based MN.IT staff did not implement controls to ensure that system development staff followed its change management plan for application development. The change management plan that department-based MN.IT staff created to support the Department of Education's significant applications did not establish expectations for:

- The segregation of privileges in existing security roles to prevent developers from introducing untested and unauthorized changes into production.

- The extent of testing required before making a change in production. Because expectations about the level of testing to be conducted was not documented prior to conducting testing, it is difficult to independently assess the adequacy of the testing.

[6] Compliance with this standard was required on April 22, 2013.

- Implementing controls designed to detect unauthorized or unlogged changes to application code.

Without sufficient controls to prevent or detect unauthorized changes to the supporting hardware and software, there is an increased risk that a change could negatively impact the applications' operations and the integrity of underlying data.

Recommendations

- *The Office of MN.IT Services should document configuration baselines in accordance with the state's Enterprise Security Configuration Management Standard.*

- *The Office of MN.IT Services, in consultation with the Department of Education, should enhance the application change management plan to better mitigate the risk of untested and unapproved changes being made to the department's applications.*

Finding 4

Servers supporting the Department of Education's significant applications were not adequately monitored for vulnerabilities.[7]

Department-based MN.IT staff had not implemented internal controls to identify, assess, and remediate potential security weaknesses on the 21 servers that supported the Department of Education's significant applications. The servers had no asset scores assigned that corresponded to the department's assessed criticality of the significant applications residing on them.[8] The asset scores help to prioritize vulnerability management efforts toward servers supporting applications that are most critical to the department.

In order to remediate security risks in the computer environment, the vulnerabilities must first be identified. Vulnerabilities are identified by using specialized software to scan the servers, called a vulnerability scanner. Providing the vulnerability scanner with a privileged user name and password, called an authenticated scan, allows the scanner to provide more detailed information about certain vulnerabilities than would be provided in an unauthenticated scan. Of the 21 servers, 6 were not being scanned for vulnerabilities and 11 were not subjected to authenticated scans.

[7] This finding is similar to a finding in a previous report: Office of the Legislative Auditor's Financial Audit Division Report 10-17, *Department of Education*, issued May 5, 2010, Finding 5.
[8] This finding is also referenced in the Office of the Legislative Auditor's Financial Audit Division Report 12-11, *Vulnerability Management*, issued May 22, 2012, Finding 1.

After vulnerabilities are identified, they must be remediated either by applying patches or other mitigating controls. Department-based MN.IT staff had not validated four critical vulnerabilities that were identified for over 120 days nor had they documented a plan to mitigate the risks created by the vulnerabilities. Five servers had high composite vulnerability scores (sum of the scores of all vulnerabilities that existed) without a plan to address the vulnerabilities or mitigate the risks created by the vulnerabilities. These deficiencies existed because department-based MN.IT staff did not consistently review the results of the vulnerability scans to ensure the effectiveness of the server patching process.

In addition, department-based MN.IT staff did not review the monthly vulnerability metrics generated by the Office of MN.IT Services with department management. The metrics show the results of scans against the standard established by the Office of MN.IT Services. These metrics allow department management to better understand, assess, and address some risks in its significant applications.

The MN.IT service level agreement requires department-based MN.IT staff to comply with the state's Enterprise Vulnerability Management Standard.[9] This standard requires the department-based MN.IT staff to, among other things, assess devices for criticality, scan all devices, resolve priority vulnerabilities within established timeframes, and review scan results to monitor resolution.

Recommendation

- *The Department of Education should ensure that the Office of MN.IT Services is providing vulnerability services in compliance with state standards and the service level agreement by:*
  - *Reviewing the monthly vulnerability management metrics.*
  - *Discussing with Office of MN.IT Services the risks created by vulnerabilities identified in the metrics.*
  - *Ensuring that the Office of MN.IT Services validates and remediates (or mitigates) vulnerabilities within timeframes identified in the standard.*

[9] Compliance with this standard was required on December 23, 2010.

Finding 5

The Department of Education lacked documented processes to authorize and review access to its significant applications' supporting hardware and software by staff from the Office of MN.IT Services.

Neither the Department of Education nor the department-based MN.IT staff established access control processes, including a periodic review of department-based MN.IT staff access to databases of the significant applications we reviewed. They also had not reviewed default access granted to system provided security roles to determine if they were appropriate, as required by the state's Enterprise Security Configuration Management Standard.

As of March 31, 2013, servers and databases supporting the department's significant applications had the following instances of inappropriate access:

1) An application login ID had excessive database privileges.
2) Department-based MN.IT staff shared login ID's to administer underlying databases without effective mitigating controls to establish accountability.
3) An administrator account's password never expired.
4) Four accounts with access to the operating systems had no established business reasons for the access.
5) One operating system and a database system did not enforce password complexity policies.

Without sufficient and timely controls to prevent and/or detect unnecessary access to databases and supporting hardware and software, there is an increased risk that the excessive access could negatively impact the Department of Education's operations and affect the integrity and confidentiality of its underlying data in key systems when exploited by authorized or unauthorized users.

Recommendation

- *The Department of Education should work with MN.IT staff assigned to the department to ensure the following:*
  - *Access rules for supporting operating systems and databases are documented.*
  - *Periodic reviews of the access to supporting operating systems and databases are performed to ensure access remains appropriate.*

Minnesota Department of Education

August 27, 2013

James Nobles
Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155-1603

Dear Mr. Nobles:

Thank you for the work done on the information technology security audit at the Department of Education.

As your report acknowledged, the designing, building, maintaining, and improving of our computerized systems would not be possible without key collaboration with management and staff from the Office of MN.IT Services. Commissioner Carolyn Parnell from MN.IT Services, and I both recognize the need to implement strong controls to protect the confidentiality, integrity and availability of educational data and systems. We appreciate your recommendations for improvements.

MN.IT Services and MDE have responded specifically to each recommendation, and those responses are contained on the following pages. Both the Minnesota Department of Education and MN.IT Services will work collaboratively to make the necessary improvements.

Once again, we thank you and the staff of the Office of the Legislative Auditor for your time and effort on this audit.

Sincerely,

Brenda Cassellius

Dr. Brenda Cassellius
Commissioner, Department of Education

Carolyn Parnell
Commissioner, Office of MN.IT Services

Finding 1

The Department of Education's significant computer applications did not have comprehensive security plans.

Response:

We concur with this finding. While the Department of Education and MN.IT Services have worked to improve the documentation of expected security and privacy controls within our systems, we also recognize that gaps do exist, particularly with our older systems. Some of our legacy systems were developed long before there was NIST guidance for system security plans. However, the newly consolidated MN.IT Services is now working to develop consistent system security plans that align with NIST for all new major government systems.

Through MN.IT Services' consolidation activities, we will prioritize the need for system security plans with available information security resources. The MN.IT Services Chief Information Security Officer will be responsible for:

- Developing and maintaining information security policies, procedures, and control techniques to address system security planning,
- Managing the identification, implementation, and assessment of common security controls,
- Ensuring that personnel with significant responsibilities for system security plans are trained,
- Assisting agency officials with their responsibilities for system security plans, and
- Identifying and coordinating common security controls for the agency.

The MN.IT Services Chief Information Officer designated for the Department of Education will be responsible for:

- Developing the system security plan in coordination with the agency business units, system administrators, the chief information security officer and security engineers,
- Maintaining the system security plan to ensures that the system is deployed and operated according to the agreed-upon security requirements,
- Ensuring that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),
- Updating the system security plan whenever a significant change occurs, and
- Assisting in the identification, implementation, and assessment of the common security controls.

The Department of Education will be responsible for:

- Providing adequate financial resources to support the appropriate level of security controls,
- Approving the system security plans and authorizing operation of its information systems,
- Establishing the rules for appropriate use and protection of the subject data/information,
- Providing input to MN.IT regarding the security requirements and security controls for the information system(s) where the information resides,
- Assisting with who has access to the information system and with what types of privileges or access rights, and
- Assisting with the identification and assessment of the common security controls where the information resides.

Finding 2

The security controls for one of the Department of Education's most important operating system were not adequate to protect not public information.

Response:

We agree with this finding. As noted in the report, the Department of Education is seeking to move away from this legacy system into a modern, cost effective operating system with more robust security capabilities. We will work with MN.IT Services to determine what control improvements can be implemented without significant system renovations and/or costs. As we modernize our operating systems and applications, we will work with MN.IT Services to design and implement security controls that are consistent with enterprise policies and standards for financial and not public data. Our MN.IT Services Chief Information Officer designated for the Department of Education will be responsible for the development of a plan of action, with specific milestones, by October 15, 2013.

Finding 3

The expected security settings were not documented for the Department of Education's significant computer applications. Also, changes to the applications could occur without complying with the change management plan.

Response:

We concur with this finding. As noted in our response to Finding 1, MN.IT Services is working with agencies to better document expected security settings within system security plans. Furthermore, to assist with setting configuration baselines, MN.IT Services contracted with the Center for Internet Security (CIS) in early 2013 to make secure configurations, together with an assessment tool, available for all state employees, including those of the Minnesota State Colleges and Universities. As agencies, including the Department of Education, begin to utilize solutions that are vetted by our newly consolidated architecture and security teams, MN.IT will have standardized configurations that will align with the CIS and other best practice or regulatory recommendations.

MN.IT Services is also working to strengthen change management practices across all agencies, including the Department of Education. As articulated in its Tactical Plan, MN.IT is working on standardization of information technology service management processes, which would include change management. With the consolidation, MN.IT will now have the opportunity to develop common controls across all agencies and will provide greater staffing flexibility such that it can better separate development, testing, and deploying changes into production. Furthermore, as MN.IT is able to better integrate security monitoring tools, it will have better insights to detect changes to applications that have not been properly tested and approved.

These consolidation and process changes will, however, take some time to implement. In the interim, MN.IT's agency-based Chief Information Officer designated for the Department of Education will be responsible for the documentation of current system configurations baselines and implementing tighter change management controls.

Finding 4

Servers supporting the Department of Education's significant applications were not adequately monitored for vulnerabilities.

Response:

We concur with this finding. As the audit report noted, this finding has been a repeat issue and MN.IT Services is currently working on resolution initiatives. Those initiatives seek to create a centralized team of dedicated and highly skilled vulnerability management professionals. This team will follow a consistent and repeatable methodology to make sure that problems get resolved in a timely manner and meet the requirements that are outlined in our policy and standard. Furthermore, as the Department of Education enhances its use of standardized MN.IT Service computing solutions; those that have predefined patching and maintenance processes, vulnerabilities can be better managed.

The MN.IT Services agency-based Chief Information Officer designated for the Department of Education will be responsible for ensuring all critical servers are being scanned in accordance with the security standards and will begin discussing vulnerability metrics with agency leaders on a quarterly basis. We anticipate resolution to be completed by December 31, 2013.

Finding 5

The Department of Education lacked documented processes to authorize and review access to significant applications' supporting hardware and software by staff from the Office of MN.IT Services.

Response:

We concur with this finding. The Department of Education allows MN.IT staff the authority to access systems and applications necessary to perform their job functions and expects that the MN.IT agency-based Chief Information Officer at the Department of Education will be accountable for the authorization and review of those privileges. The Department of Education will work closely with its agency-based CIO to annually review privileged access to its systems. We anticipate resolution to be completed by June 30, 2014.