Claire McCaskill
Missouri State Auditor

August 2005

HEALTH AND SENIOR SERVICES

Information Technology Security Controls

Report no. 2005-59 **auditor.mo.gov**

Claire McCaskill
Missouri State Auditor

YELLOW SHEET

Sensitive Health Department data is vulnerable to unauthorized use, and department computer security is not in full compliance with federal rules

This audit reviewed the computer security management program at the Department of Health and Senior Services (DHSS). Auditors assessed if computer security efforts ensured department data remained confidential and complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule by the federal deadline. The following highlights the audit findings.

Partially implemented security program leaves data at risk

DHSS did not have a fully developed security management program. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. (See page 5)

Risk assessment process not fully implemented

DHSS had not fully implemented a formal risk assessment process or had policies to conduct such assessments, although informal risk assessments are regularly performed. Risk assessments need to be documented and the HIPAA Security Rule states risk assessments are necessary to protect data confidentiality and integrity. (See page 6)

No requirement to confirm user access rights

DHSS management did not require periodic confirmation of user access rights. Such review would ensure access rights are commensurate with the user's job duties. (See page 9)

Reinvestigation of employee backgrounds not performed

DHSS had not reinvestigated backgrounds of employees in technology positions. Accepted standards call for reinvestigations every 5 years. (See page 9)

Not fully compliant with federal security rules

The HIPAA Security Rule required health information be secured by April 2005. DHSS did not meet this deadline, although officials did comply with several parts of the Security Rule. HIPAA includes provision for fines of $100 per violation for non-compliance with Act requirements. (See page 11)

Default password settings leave system vulnerable

Auditors found password settings to gain access to some systems were left at default settings, which did not comply with department security policies or accepted standards. Information systems staff said resetting the passwords was not a priority due to the limited number of users for the applicable systems. (See page 12)

All reports are available on our website: auditor.mo.gov

CLAIRE McCASKILL

Missouri State Auditor

Honorable Matt Blunt, Governor
and
Julia M. Eckstein, Director
Department of Health and Senior Services
Jefferson City, MO 65102

The Department of Health and Senior Services' (DHSS) mission is to protect and promote quality of life and health for all Missourians by developing and implementing programs and systems that provide information and education; effective regulation and oversight; quality services; and surveillance of diseases and conditions. DHSS's Office of Information Systems (OIS) is responsible for providing computer systems to support this mission. Our objectives included determining whether DHSS management (1) established adequate information technology security controls to ensure the confidentiality, integrity, and availability of data and information and (2) complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule by the federal deadline.

We found DHSS had not fully implemented a security management program to protect the information and technology assets that support the mission and operations of the department. We identified weaknesses in existing security policies and procedures and instances where critical security policies had not been developed. While we identified information technology security controls that had been developed and implemented, DHSS had not implemented all of the standards and specifications required to be in compliance with the HIPAA Security Rule. We also determined DHSS had not established a strategic plan for technology to ensure technology resources are integrated with the department's overall mission and business goals. In addition, we found weak security settings over some passwords, which increase the risk that data or systems could be compromised.

We have included recommendations to improve information technology security controls, which should help DHSS ensure the confidentiality, integrity, and availability of data and information.

We conducted our work in accordance with Government Auditing Standards issued by the Comptroller General of the United States. This report was prepared under the direction of Kirk Boyer. Key contributors to this report included Jeff Thelen, Lori Melton, Frank Verslues and Preston Hammond.

Claire McCaskill

Claire McCaskill
State Auditor

Contents

Sensitive Data and Systems Are Vulnerable to Unauthorized Use and Disclosure 3

Background 3

Scope and Methodology 4

Security Management Program Is Not Fully Implemented 5

DHSS Is Not Fully Compliant With HIPAA Security Rule 11

DHSS Lacks Strategic Plan for Technology 11

Default Password Security Settings Leave Some DHSS Systems Vulnerable 12

Conclusions 12

Recommendations 13

Agency Comments 14

Appendix I Agency Comments 15

Abbreviations

DHSS	Department of Health and Senior Services
GAO	Government Accountability Office
HIPAA	Health Insurance Portability and Accountability Act of 1996
OIS	Office of Information Systems

Sensitive Data and Systems Are Vulnerable to Unauthorized Use and Disclosure

Technology assets and information that is processed, stored, and transmitted on Department of Health and Senior Services' (DHSS) systems may be inadequately protected from unauthorized disclosure, modification, use, or destruction. This situation has occurred because DHSS had not fully implemented a security management program to protect the information and technology assets that support the mission and operations of the department. Without the guidance of a security management program, information technology security policies and procedures had not been developed or were missing key elements. While some information technology security controls had been developed and implemented, DHSS had not implemented all of the standards and specifications required to be in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. DHSS also has not established a strategic plan for technology to ensure technology resources are used for department priorities and are integrated with the department's overall strategic objectives. In addition, password security settings for some DHSS systems had been left at default settings which increases the risk that data or systems could be compromised. Collectively, these weaknesses impair DHSS's ability to ensure the confidentiality, integrity, and availability of data and sensitive health information.

Background

DHSS is responsible for protecting and promoting the health of all Missourians. According to its mission statement, DHSS attempts to meet this responsibility by developing and implementing programs and systems that provide information and education; effective regulation and oversight; quality services; and surveillance of diseases and conditions.

To administer its programs, DHSS must assure clients and providers the confidentiality and privacy of health care information the department electronically collects, maintains, uses, or transmits is secure. Security of health information is especially important when such information can be directly linked to an individual. Confidentiality is threatened not only by the risk of improper access to electronically stored information but also by the risk of interception during electronic transmission of the information.

The Office of Information Systems (OIS) oversees the management of all computer programs and systems for DHSS. Information, some of which is sensitive, maintained in DHSS systems includes:

- Childhood lead poisoning prevention program
- Communicable and environmental disease prevention, treatment reporting, and investigation
- Elderly abuse hotline
- Food establishment inspections and licenses

- Health care employee disqualification list
- Immunization records
- Organ donor records
- Various licensing and inspection information, such as for child/adult day care facilities or health facilities
- Vital records
- Other health statistics

In April 2005, DHSS transferred the job duties of the Security Officer to the Chief Information Officer. Those duties included maintenance of DHSS security policies and procedures, development of an information security awareness program, and ensuring appropriate and cost-effective security control measures are in place for all information systems.

HIPAA requires, among other provisions, health plans and providers to protect and secure certain health information. The safeguards comprising HIPAA-mandated security focus on protecting data confidentiality, integrity, and availability of individually identifiable health information. When Congress legislated HIPAA in 1996, it required compliance within 18 months. The federal Department of Health and Human Services proposed a HIPAA Security Rule to supplement the law in 1998. This HIPAA Security Rule was finalized in April 2003 and required compliance by April 2005. DHSS evaluated its systems and determined some of the systems fall under this rule. Since many of the provisions of the HIPAA Security Rule are for general security, the entire department must follow the HIPAA Security Rule standards and specifications.

According to accepted standards, computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of information system resources.

Scope and Methodology

To understand DHSS information technology security controls, we identified and reviewed department and OIS policies and procedures, user manuals, and other documents. We also discussed with the Chief Information Officer, the Security Officer, and other key OIS staff whether information technology security controls were in place and operating effectively.

To determine compliance with the HIPAA Security Rule, we reviewed the regulation and underlying law and the HIPAA Security Rule. We compared DHSS policies and procedures to the HIPAA Security Rule standards and specifications.

We based our evaluation on applicable federal, national and international standards and best practices related to information technology security controls from the following sources:

- National Institute of Standards and Technology
- Information Systems Audit and Control Association
- U.S. Government Accountability Office (GAO)

We also reviewed the Missouri Adaptive Enterprise Architecture developed and maintained by the Office of Administration's Information Technology Services Division to determine whether statewide security standards had been established and finalized. We specifically reviewed the partially finalized security domain, which defines the standards and policies needed to protect the information and technology assets of the state.

We requested comments on a draft of our report from the Director of the Department of Health and Senior Services, and those comments are reprinted in Appendix I. We conducted our work between February and June 2005.

Security Management Program Is Not Fully Implemented

A security management program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. A security management program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. Implementing an information security program is essential to ensuring controls over information and information systems work effectively on a continuing basis, according to GAO.

DHSS had not fully established a security management program on which department-wide security policies, standards, and procedures can be formulated, implemented, or monitored. OIS management stated DHSS adopted the Missouri Adaptive Enterprise Architecture security domain as its architecture framework. The security domain is not fully developed, but it defines the security management principles which are needed to ensure the appropriate level of protection for the state's information and technology assets. When completed, the security domain architecture will provide a security plan template for agencies to use as guidance when developing agency plans; it will not provide an actual plan for agencies to implement.

Although the security domain architecture is not fully developed, standards are available to DHSS for security management planning. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. According to GAO, a critical element of an effective security management program is developing and implementing policies and procedures to govern security over an agency's information technology environment.

DHSS has developed and documented policies for specific security areas, including password standards and business continuity planning. However, policies and procedures still need to be developed for the following areas:

- Risk assessment program
- System and data classification
- Security activity and violation logging and review
- Review of security settings
- Segregation of duties
- User account access rights review
- Position sensitivity analysis and background reinvestigations
- Security incident handling and reporting
- Security awareness training

Risk assessment program is not fully implemented

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure policies and controls operate as intended, according to GAO. A risk assessment helps to identify potential vulnerabilities and threats or weaknesses that could be exploited and to ensure appropriate controls are implemented to mitigate these vulnerabilities.

DHSS had not fully implemented a formal risk assessment process and had no policies for conducting these assessments. OIS management said a formal risk assessment has never been performed. The Chief Information Officer said however, that informal, undocumented risk assessments are performed regularly. Since risks and threats change over time or employees leave, the results of risk assessments need to be documented to ensure an appropriate action plan is developed to limit vulnerabilities. According to the HIPAA Security Rule and accepted standards, an assessment of the potential risks and vulnerabilities is necessary to protect the confidentiality, integrity and availability of data and information.

Systems and data not classified according to sensitivity and criticality

DHSS management does not have assurance systems and data receive an appropriate level of protection. DHSS had not established a department-wide framework for systems and data classification, according to OIS management. Such a framework examines the sensitivity of both the data to be processed and the system itself to identify when to classify information as confidential, public, or other established levels.

A general classification framework is established to define an appropriate set of protection levels and the placement of data in information classes, according to accepted standards. Sensitivity is generally classified in terms of confidentiality, integrity, and availability. Factors such as the importance of the system to the organization's mission and the consequences of unauthorized use of the system or data need to be examined when assessing sensitivity. OIS management said a classification framework had not been developed because the department was waiting for policy from the Office of Administration Information Technology Services Division in this area. The Information Technology Services Division issued a draft standard on data classification in January 2005, but the state's Chief Information Officer said there are plans to revise this document and does not know when it will be finalized.

Policies needed to log, report and review security activity and violations

DHSS management had not taken sufficient steps to ensure system security controls have functioned properly. Policies and procedures for logging appropriate security-related events and monitoring specific access are necessary when developing effective security programs. Accepted standards state security activity[1] should be logged, reported, reviewed and appropriately evaluated on a regular basis to identify and resolve incidents involving unauthorized activity. In addition, the HIPAA Security Rule requires procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

A properly functioning security monitoring program is essential to ensure unauthorized attempts to access critical data are detected and investigated, according to GAO. A security monitoring program would include routinely reviewing security violations including failed attempts to access sensitive data and resources. These actions are critical for ensuring improper access to sensitive information is detected on a timely basis.

[1] Security activity includes users attempting to access data they are not authorized to access, performing a task they are not authorized to perform, or accessing data they are authorized to access that is of a sensitive nature.

Policies needed to report and review security settings

Agencies help secure networks by installing and configuring a network operating system, security software, and network devices[2] that permit authorized activity and deny unauthorized requests. Since sensitive data and programs are stored on or transmitted along networks, adequately securing networks is critical to protect data and information technology resources from unauthorized access and use.

DHSS has not developed policies to review security settings for the network server operating system, network security software, or the network devices. OIS management stated there are no formally documented procedures for periodically reporting and reviewing security settings for these network systems and devices. However, OIS management said security settings are reviewed and tested before the network devices are put in use. According to accepted standards, monitoring alterations of system security settings is important to ensure changes did not diminish security.

OIS management said reviews have not been necessary because trusted employees have access to make changes and do not need to be monitored. However, security settings could still be overlooked. According to the GAO, a key element of a security management program is ongoing testing and evaluation to ensure systems are in compliance with policies, and that policies and controls are both appropriate and effective. This type of oversight is a fundamental element because it demonstrates management’s commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness.

Policies needed to ensure segregation of duties

Inadequately segregated duties increase the risk erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed, according to GAO. DHSS had not created or implemented a policy requiring segregation of duties among information technology staff, according to OIS management. In addition, DHSS had no policies in place to review logical access to ensure adequate segregation of duties. OIS management agreed segregation of duties should be ensured, but stated DHSS relies on the inherent segregation imposed by the divisions within the organizational chart. We could not verify whether segregation has been sufficient without a comprehensive list of user account access rights, which was not available (see next section). Accepted standards state policies should be established to require a division of roles

[2] Network devices include (1) firewalls to prevent unauthorized access into the network, (2) routers to filter and forward data through the network, and (3) switches to forward data among parts of the network.

and responsibilities that should exclude the possibility for a single individual to subvert a critical process.

Review of user account access rights needed

Monitoring users and their access rights is an on-going process. User access may change permanently or temporarily. Without complete and timely reporting of user access, management cannot ensure users' access is limited to only those functions necessary to accomplish assigned job responsibilities or ensure unauthorized changes of user access rights will be detected, according to accepted standards. These accepted standards state a review of users and access rights should examine the levels of access each individual has, if the access is needed to perform their duties, whether all accounts are still active, and whether management authorizations are up-to-date.

OIS management said DHSS had no policies or procedures requiring management to review and confirm all user access rights periodically. Additionally, system administration did not have a process in place for reporting all DHSS user access rights so they can be reviewed by the resource owners to ensure access rights are commensurate with the user's job duties and responsibilities.

Each system and application DHSS maintains has the capability to report user access, according to OIS management. However, there is no single list of users with all their access rights. In order for OIS to create a comprehensive list of users and access rights, system administration would have to compile user access information from all the various systems and applications. OIS is currently working on integrating the user access reporting capabilities of all DHSS systems, according to OIS management. The purpose of the new program is to provide resource owners with a complete listing of users and access rights. Once the integration is complete, user access rights will be pulled directly from the various systems and reported directly to the resource owners for review. However, personnel funding issues for integrating the new automated security access program are currently prohibiting OIS from dedicating the personnel necessary to complete the project, according to OIS management.

Background reinvestigations of employees in sensitive technology positions not performed

DHSS management risks not detecting unacceptable employee actions because background reinvestigations have not been performed on current employees in technology positions. DHSS policy requires background investigations for applicants being offered a job with the department. Background screenings help determine whether an individual is suitable for a given position.

According to accepted standards, periodic background reinvestigations should be performed at least once every 5 years, consistent with the sensitivity of the position. However, DHSS management said the department has not reviewed positions to determine sensitivity. Sensitivity levels are based on the type and degree of harm, such as disclosure of confidential information, an employee can cause through the misuse of computer systems and its data. Sensitivity levels are used to determine if job positions require background screenings. Without determining levels of sensitivity of job positions, management cannot establish which positions need reinvestigations.

Security incident handling procedures not fully documented

DHSS had no comprehensive procedures to address computer security incident handling and had not documented incident handling responsibilities and duties. Computer security incident handling and response is the process and actions an organization takes in response to a computer security incident, according to accepted standards.[3]

An incident response policy should be created as a foundation for incident response procedures, according to accepted standards. DHSS's policy lacked key components, including a means for prioritizing incidents and responsibilities for handling and tracking incidents. The HIPAA Security Rule also requires covered entities to implement policies and procedures to address reasonably anticipated security incidents that pose a threat or hazard to the security or integrity of protected information.

The responsibilities and procedures related to incident handling have been incorporated into employees' daily job duties, according to OIS management. However, we found these responsibilities and procedures have not been formally documented. Without formally documented procedures, there are no guidelines to ensure the priorities of the organization are reflected in response operations to consistently handle security incidents, according to accepted standards. As a result, incidents may not be handled in the most optimal manner, leaving the network or other systems vulnerable.

Employees had not received ongoing security awareness training

Training is an essential component of a security management program. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital employees using computer resources be aware of the importance and sensitivity of information handled, as well as business and legal rationale for

[3] The Office of Administration Information Technology Services Division defines a security incident as an adverse event, or threat of an adverse event, in a computer system and/or network.

maintaining its confidentiality, integrity, and availability, according to GAO.

DHSS management said personnel had not been trained on an ongoing basis regarding computer security and their roles in ensuring appropriate use of department resources. New employees received security training as part of orientation, but employees received no other security awareness training except sporadic reminders when a problem occurred. According to accepted standards, employees play a crucial role in helping ensure the security of computer systems and information technology resources. Accepted standards also state ongoing training programs are necessary to maintain employees' security awareness to the level required to perform effectively. In addition, the HIPAA Security Rule required a security awareness and training program for all employees be implemented by the April 2005 deadline.

The Chief Information Officer said a computer-based training program has been established to comply with the HIPAA Security Rule and all staff are required to take it. We found the training included information related to DHSS's security issues and had been made available for employees in June 2005.

DHSS Is Not Fully Compliant With HIPAA Security Rule

The HIPAA Security Rule required health plans and providers ensure safeguards be taken to protect the security of health information by April 2005. DHSS did not comply with the HIPAA Security Rule by the federal deadline. However, we found the department did comply with parts of the HIPAA Security Rule and the following had been established:

- Business continuity and disaster recovery plans.
- Policy for sanctioning employees who fail to comply with the security policies and procedures.
- Procedures authorizing access to electronic protected health information, or in locations where it might be accessed.
- Administrative rules for terminating access.
- Policies and procedures for creating, changing, and safeguarding passwords.

Section 1176 of HIPAA provides penalties of $100 per violation, not to exceed $25,000 a year for violations of an identical requirement or prohibition, for non-compliance with the Act.

DHSS Lacks Strategic Plan for Technology

Technology planning is the process of establishing goals and objectives, developing strategies to achieve those objectives, and developing plans to ensure the strategies are implemented. Technology plans help ensure costly technology investments are focused in the areas of greatest strategic importance. This process ensures the effectiveness of those investments by matching information technology priorities to an organization's overall priorities, as explained in *State and Local Government Information Security – Operations and Technical Management*.[4]

DHSS did not have a strategic plan to align its information technology resources with its overall mission and business goals. Although DHSS prepares an overall strategic plan, the Chief Information Officer stated he had not been involved in the department's business planning process. The Chief Information Officer did provide a technology report that lists the previous year's accomplishments and planned projects for upcoming years. However, this report did not address the department's goals, how technology is used to help attain these goals, or priorities of planned projects. According to accepted standards, technology plans should be developed to help ensure the use of technology is aligned with the mission and goals of the organization.

The DHSS Chief Information Officer stated there are processes in place, including the establishment of an Information Technology Advisory Committee, to facilitate the technology planning process. DHSS established the Information Technology Advisory Committee to review policies, make recommendations on department business priorities, and to help ensure technology issues are communicated throughout the department.

Default Password Security Settings Leave Some DHSS Systems Vulnerable

DHSS policy requires passwords be at least 5 characters and reset at least every 60 days, and user accounts be locked after 42 days of inactivity. However, we found password security settings for some DHSS systems had been left at default settings, which did not comply with DHSS policy or accepted standards. OIS management said they were aware of these settings and agreed passwords should be in compliance with DHSS policy. However, OIS management added changing default settings had not been a priority because there have been a limited number of users for the applicable systems.

Conclusions

DHSS has not effectively implemented some critical information technology security controls to properly protect the confidentiality, integrity, and availability of data and sensitive health information processed by the department's computers and network. Weaknesses exist in DHSS's information security controls because it has not fully implemented a

[4] *State and Local Government Information Security – Operations and Technical Management*, Version 2.0, Geoffrey H. Wold and Jeffrey S. Locketz, December 2002.

comprehensive security management program to ensure effective controls are established and maintained, and information security receives significant management attention. Until DHSS fully implements a security management program and takes steps to develop the necessary policies and controls to correct or mitigate its information security control weaknesses, DHSS will have limited assurance its sensitive information and systems are adequately protected. Specifically, DHSS has not developed policies to (1) implement a risk assessment program; (2) classify systems and data according to sensitivity; (3) log and report security activity and violations; (4) periodically report and review security settings for network server operating system, security software, and other network devices; and (5) ensure adequate segregation of duties. In addition, the lack of (1) periodic reviews of user access rights, (2) determining which employee technology positions are highly sensitive and need background reinvestigations, (3) fully documented procedures and responsibilities for handling and tracking computer security incidents, and (4) an ongoing employee security awareness program, increases the level of risk.

While some information technology security controls were in place, DHSS has not developed and implemented all of the standards and specifications required to be in compliance with the HIPAA Security Rule. As a result, DHSS cannot ensure the confidentiality, integrity, and availability of protected health information. To strive towards compliance with the HIPAA Security Rule, DHSS needs to develop the policies and procedures necessary to fully implement its security management program.

DHSS did not have a strategic plan for technology in place. A structured planning approach should help DHSS establish goals and objectives, define strategies and policies to help achieve those objectives, and develop a detailed technology plan to ensure the strategies are properly implemented. Without a technology plan in place, DHSS cannot guarantee the integration of information technology initiatives with the department-wide strategic business plan.

Password security settings for some systems have been left at the default settings, which does not comply with DHSS policy or accepted standards. This weakness increases the risk of passwords being compromised and unauthorized transactions going undetected.

Recommendations

We recommend the Director of the Department of Health and Senior Services:

1. Enhance existing security controls by fully developing a comprehensive security management program to protect the confidentiality, integrity, and

availability of data and systems and to protect the security of health information required by the HIPAA Security Rule. Management should develop policies and procedures and implement security controls by taking the following actions:

- Fully implement a risk assessment program and policy,
- Establish a systems and data classification framework,
- Develop policies and procedures to log, report, and review appropriate security activity and security violations,
- Develop policies to periodically report and review network security settings,
- Develop policies to ensure adequate segregation of duties,
- Perform a periodic review of user account access rights,
- Evaluate employee technology positions for sensitivity to determine which positions are highly sensitive and need background reinvestigations,
- Fully document security incident handling procedures and responsibilities, and
- Implement an ongoing employee security awareness and training program.

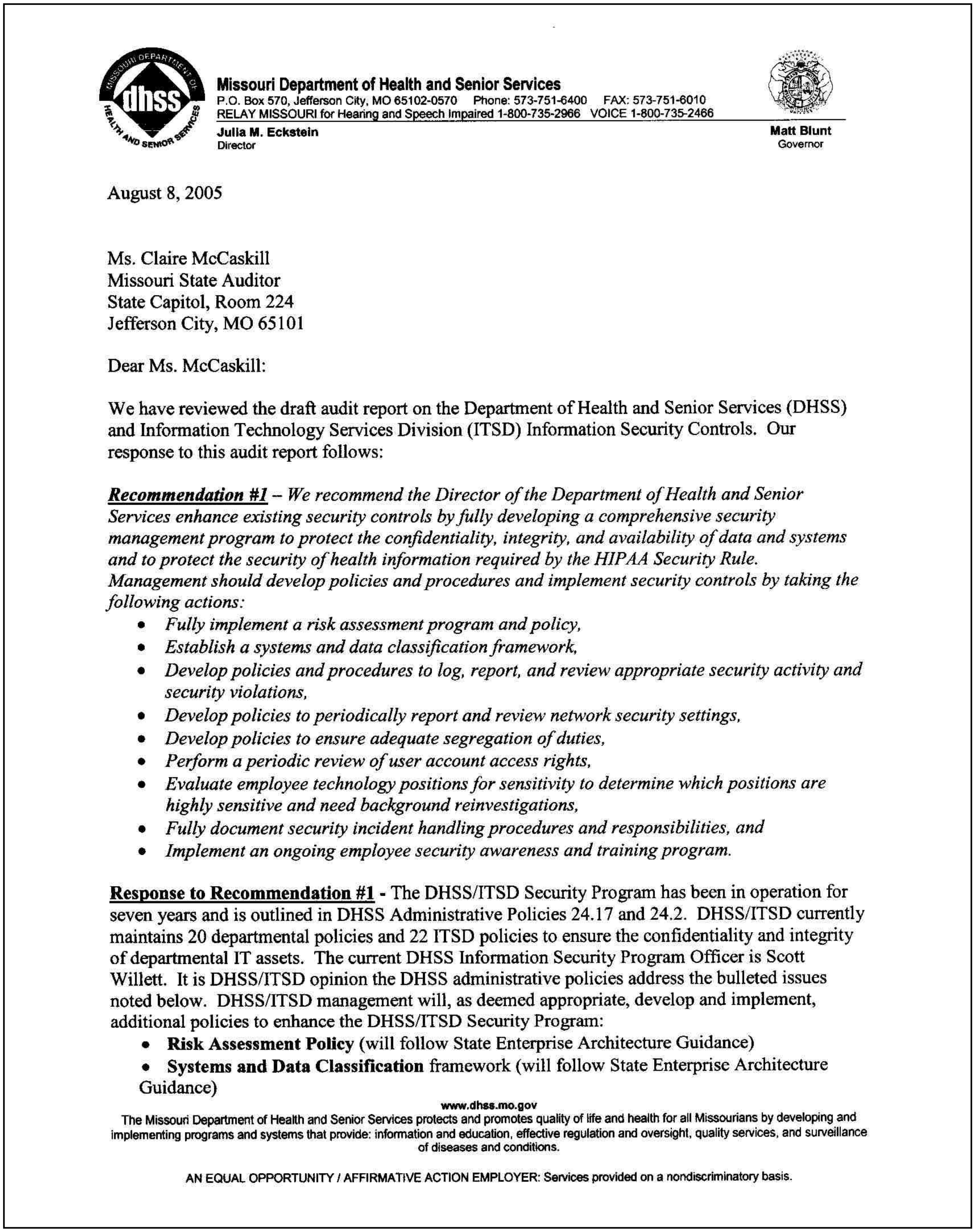
2. Develop a strategic plan for technology to support the department's goals and incorporate technology issues in the department's overall strategic planning process.

3. Ensure all password security settings comply with department policy and accepted standards.

Agency Comments

See Appendix I for agency comments.

Agency Comments



Missouri Department of Health and Senior Services
P.O. Box 570, Jefferson City, MO 65102-0570 Phone: 573-751-6400 FAX: 573-751-6010
RELAY MISSOURI for Hearing and Speech Impaired 1-800-735-2966 VOICE 1-800-735-2466

Julia M. Eckstein
Director

Matt Blunt
Governor

August 8, 2005

Ms. Claire McCaskill
Missouri State Auditor
State Capitol, Room 224
Jefferson City, MO 65101

Dear Ms. McCaskill:

We have reviewed the draft audit report on the Department of Health and Senior Services (DHSS) and Information Technology Services Division (ITSD) Information Security Controls. Our response to this audit report follows:

Recommendation #1 *– We recommend the Director of the Department of Health and Senior Services enhance existing security controls by fully developing a comprehensive security management program to protect the confidentiality, integrity, and availability of data and systems and to protect the security of health information required by the HIPAA Security Rule. Management should develop policies and procedures and implement security controls by taking the following actions:*

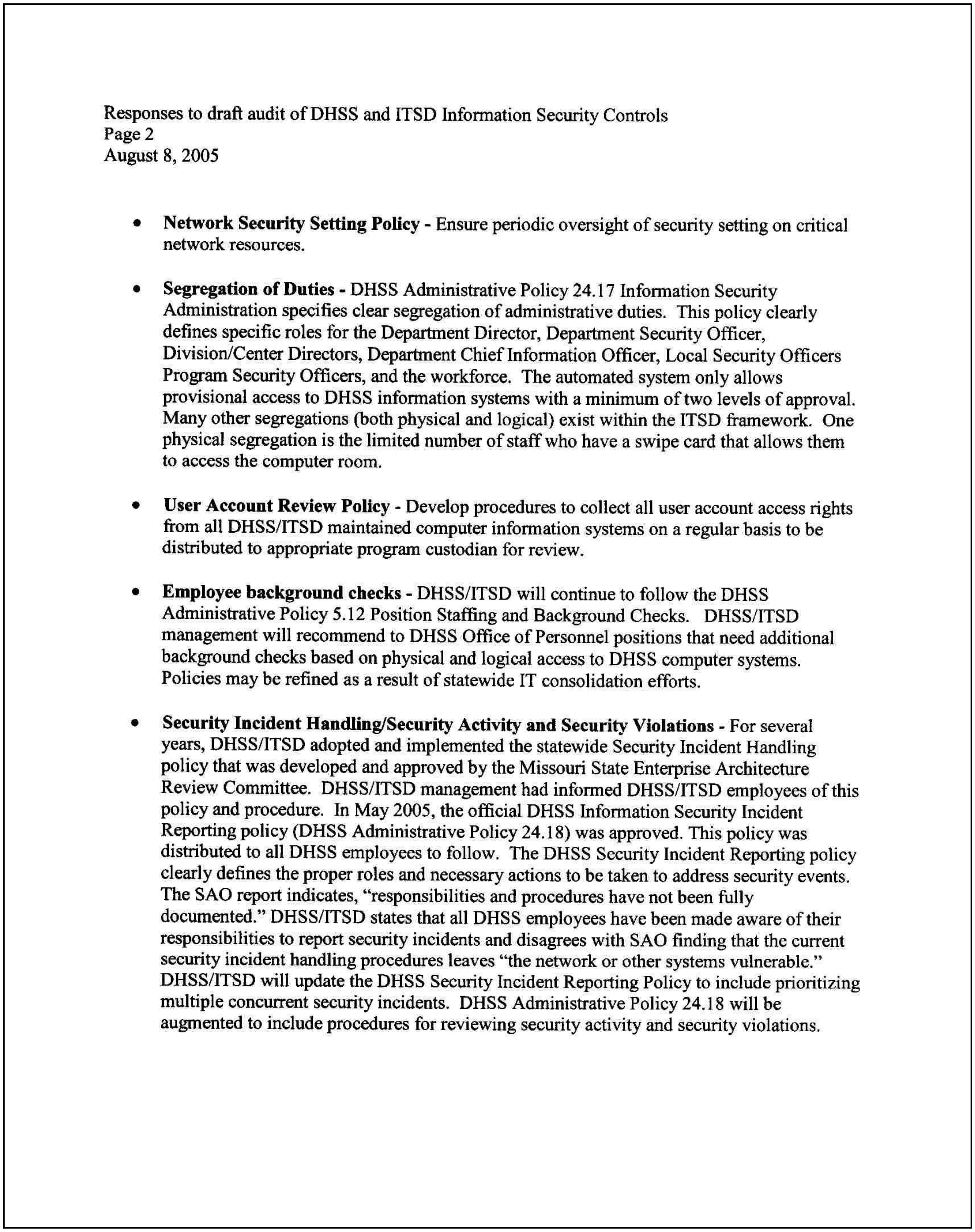
- *Fully implement a risk assessment program and policy,*
- *Establish a systems and data classification framework,*
- *Develop policies and procedures to log, report, and review appropriate security activity and security violations,*
- *Develop policies to periodically report and review network security settings,*
- *Develop policies to ensure adequate segregation of duties,*
- *Perform a periodic review of user account access rights,*
- *Evaluate employee technology positions for sensitivity to determine which positions are highly sensitive and need background reinvestigations,*
- *Fully document security incident handling procedures and responsibilities, and*
- *Implement an ongoing employee security awareness and training program.*

Response to Recommendation #1 - The DHSS/ITSD Security Program has been in operation for seven years and is outlined in DHSS Administrative Policies 24.17 and 24.2. DHSS/ITSD currently maintains 20 departmental policies and 22 ITSD policies to ensure the confidentiality and integrity of departmental IT assets. The current DHSS Information Security Program Officer is Scott Willett. It is DHSS/ITSD opinion the DHSS administrative policies address the bulleted issues noted below. DHSS/ITSD management will, as deemed appropriate, develop and implement, additional policies to enhance the DHSS/ITSD Security Program:

- **Risk Assessment Policy** (will follow State Enterprise Architecture Guidance)
- **Systems and Data Classification** framework (will follow State Enterprise Architecture Guidance)

www.dhss.mo.gov
The Missouri Department of Health and Senior Services protects and promotes quality of life and health for all Missourians by developing and implementing programs and systems that provide: information and education, effective regulation and oversight, quality services, and surveillance of diseases and conditions.

AN EQUAL OPPORTUNITY / AFFIRMATIVE ACTION EMPLOYER: Services provided on a nondiscriminatory basis.



Responses to draft audit of DHSS and ITSD Information Security Controls
Page 2
August 8, 2005

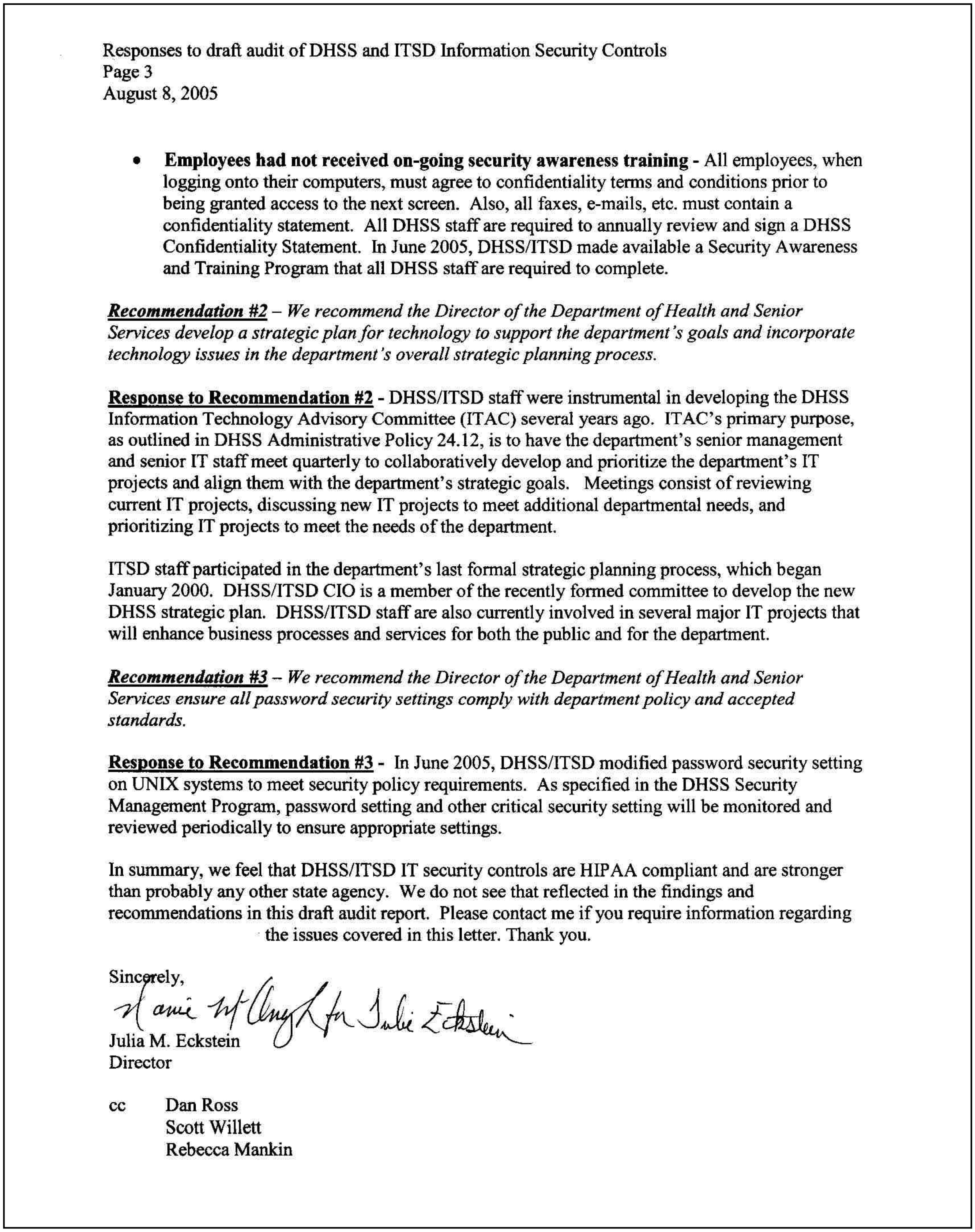
- **Network Security Setting Policy -** Ensure periodic oversight of security setting on critical network resources.

- **Segregation of Duties -** DHSS Administrative Policy 24.17 Information Security Administration specifies clear segregation of administrative duties. This policy clearly defines specific roles for the Department Director, Department Security Officer, Division/Center Directors, Department Chief Information Officer, Local Security Officers Program Security Officers, and the workforce. The automated system only allows provisional access to DHSS information systems with a minimum of two levels of approval. Many other segregations (both physical and logical) exist within the ITSD framework. One physical segregation is the limited number of staff who have a swipe card that allows them to access the computer room.

- **User Account Review Policy** - Develop procedures to collect all user account access rights from all DHSS/ITSD maintained computer information systems on a regular basis to be distributed to appropriate program custodian for review.

- **Employee background checks -** DHSS/ITSD will continue to follow the DHSS Administrative Policy 5.12 Position Staffing and Background Checks. DHSS/ITSD management will recommend to DHSS Office of Personnel positions that need additional background checks based on physical and logical access to DHSS computer systems. Policies may be refined as a result of statewide IT consolidation efforts.

- **Security Incident Handling/Security Activity and Security Violations -** For several years, DHSS/ITSD adopted and implemented the statewide Security Incident Handling policy that was developed and approved by the Missouri State Enterprise Architecture Review Committee. DHSS/ITSD management had informed DHSS/ITSD employees of this policy and procedure. In May 2005, the official DHSS Information Security Incident Reporting policy (DHSS Administrative Policy 24.18) was approved. This policy was distributed to all DHSS employees to follow. The DHSS Security Incident Reporting policy clearly defines the proper roles and necessary actions to be taken to address security events. The SAO report indicates, "responsibilities and procedures have not been fully documented." DHSS/ITSD states that all DHSS employees have been made aware of their responsibilities to report security incidents and disagrees with SAO finding that the current security incident handling procedures leaves "the network or other systems vulnerable." DHSS/ITSD will update the DHSS Security Incident Reporting Policy to include prioritizing multiple concurrent security incidents. DHSS Administrative Policy 24.18 will be augmented to include procedures for reviewing security activity and security violations.



Responses to draft audit of DHSS and ITSD Information Security Controls
Page 3
August 8, 2005

- **Employees had not received on-going security awareness training** - All employees, when logging onto their computers, must agree to confidentiality terms and conditions prior to being granted access to the next screen. Also, all faxes, e-mails, etc. must contain a confidentiality statement. All DHSS staff are required to annually review and sign a DHSS Confidentiality Statement. In June 2005, DHSS/ITSD made available a Security Awareness and Training Program that all DHSS staff are required to complete.

Recommendation #2 *– We recommend the Director of the Department of Health and Senior Services develop a strategic plan for technology to support the department's goals and incorporate technology issues in the department's overall strategic planning process.*

Response to Recommendation #2 - DHSS/ITSD staff were instrumental in developing the DHSS Information Technology Advisory Committee (ITAC) several years ago. ITAC's primary purpose, as outlined in DHSS Administrative Policy 24.12, is to have the department's senior management and senior IT staff meet quarterly to collaboratively develop and prioritize the department's IT projects and align them with the department's strategic goals. Meetings consist of reviewing current IT projects, discussing new IT projects to meet additional departmental needs, and prioritizing IT projects to meet the needs of the department.

ITSD staff participated in the department's last formal strategic planning process, which began January 2000. DHSS/ITSD CIO is a member of the recently formed committee to develop the new DHSS strategic plan. DHSS/ITSD staff are also currently involved in several major IT projects that will enhance business processes and services for both the public and for the department.

Recommendation #3 *– We recommend the Director of the Department of Health and Senior Services ensure all password security settings comply with department policy and accepted standards.*

Response to Recommendation #3 - In June 2005, DHSS/ITSD modified password security setting on UNIX systems to meet security policy requirements. As specified in the DHSS Security Management Program, password setting and other critical security setting will be monitored and reviewed periodically to ensure appropriate settings.

In summary, we feel that DHSS/ITSD IT security controls are HIPAA compliant and are stronger than probably any other state agency. We do not see that reflected in the findings and recommendations in this draft audit report. Please contact me if you require information regarding the issues covered in this letter. Thank you.

Sincerely,

Marie McClung for Julie Eckstein

Julia M. Eckstein
Director

cc Dan Ross
Scott Willett
Rebecca Mankin