

Audit Report

**Department of Public Safety and Correctional Services
Information Technology and Communications Division**

January 2016



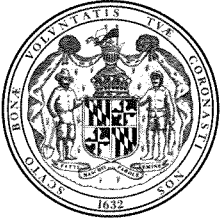
OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Warren G. Deschenaux
Executive Director

January 6, 2016

Thomas J. Barnickel III, CPA
Legislative Auditor

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee
Delegate Craig J. Zucker, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Department of Public Safety and Correctional Services (DPSCS) – Information Technology and Communications Division (ITCD). Our audit included an internal control review of the DPSCS data center and the network administered by the ITCD that supports both ITCD and DPSCS. ITCD provides computing and network resources and operates as a computer services bureau for DPSCS.

Our audit disclosed that appropriate safeguards were not established to protect sensitive information maintained in a critical database. In addition, controls over the monitoring of security events on critical databases and the mainframe computer system were not sufficient. Finally, the network administered by ITCD was not adequately secured against external threats.

DPSCS' response to this audit, on behalf of ITCD, is included as an appendix to this report.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Background Information	4
Agency Responsibilities	4
Status of Findings From Preceding Audit Report	4
Findings and Recommendations	5
Network and Data Center Information Systems Security and Control	
Finding 1 –Personally Identifiable Information Was Not Appropriately Safeguarded	5
Finding 2 – Procedures for Logging and Monitoring Critical Database and Mainframe Security Events Were Not Sufficient	5
* Finding 3 – The DPSCS Network Was Not Properly Secured	6
Audit Scope, Objectives, and Methodology	8
Agency Response	Appendix

* Denotes item repeated in full or part from preceding audit report

Background Information

Agency Responsibilities

The Information Technology and Communications Division (ITCD) of the Department of Public Safety and Correctional Services (DPSCS) operates the DPSCS data center as a computer service provider for DPSCS operating agencies (for example, the Central Region). ITCD provides data, information, and communications services to DPSCS, criminal justice entities, and the public. In addition, ITCD maintains application systems containing sensitive information, such as the Sex Offender Registry Database and the Maryland Automated Fingerprint Identification System, and operates a statewide computer network.

Furthermore, ITCD operates a wide area network (WAN) that connects with more than 300 statewide remote sites, such as local law enforcement agencies, and the DPSCS data center's local network. DPSCS, through its WAN, offers its users access to various information technology services including mainframe computer-based applications (for example, the Criminal Justice Information System), database management, network services, email, and the Internet. Finally, ITCD maintains the mainframe operating system and security software environment in which many agency applications are executed. ITCD's fiscal year 2015 budget totaled approximately \$36 million and provided funding for 214 authorized positions.

Our audit focused exclusively on the computer and network operations of the ITCD data center. An audit of the ITCD fiscal operations was conducted as part of the audit of the DPSCS Office of the Secretary, and a separate report was issued on November 18, 2015.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the three findings contained in our preceding audit report dated January 6, 2012. We determined that ITCD satisfactorily addressed two of the findings. The remaining finding is repeated in this report.

Findings and Recommendations

Network and Data Center Information Systems Security and Control

Finding 1

The Information Technology and Communications Division (ITCD) did not appropriately safeguard sensitive personally identifiable information.

Analysis

ITCD inappropriately stored sensitive personally identifiable information (PII) in clear text. Specifically, as of February 27, 2015, we identified a critical database containing 2,562,700 unique social security numbers (SSNs) along with names, and dates of birth in clear text. In addition, we determined that this sensitive PII was not protected by other substantial mitigating controls.

This PII, which is commonly sought by criminals for use in identity theft, should be protected by appropriate information system security controls. The State of Maryland's *Information Security Policy* states that agencies should protect confidential data using encryption technologies and/or other substantial mitigating controls.

Recommendation 1

We recommend that ITCD

- a. perform an inventory of its systems and identify all sensitive PII,**
- b. determine if it is necessary to retain this PII and delete all unnecessary PII,**
- c. determine if all necessary PII is properly protected by encryption or other substantial mitigating controls, and**
- d. use approved encryption methods to encrypt all sensitive PII not otherwise properly protected.**

Finding 2

Procedures for logging and monitoring critical database and mainframe security events were not sufficient.

Analysis

Procedures for logging and monitoring critical database and mainframe security events were not sufficient.

- For a critical production database, the use of numerous powerful system privileges (for example, create role and update any table) and direct changes to significant data and security tables were not logged. Accordingly, unauthorized changes to this database could occur, that could result in inappropriate changes to production data without detection by management.
- Documented reviews of reports of critical security events for the mainframe security software and two significant production databases did not exist. Although ITCD advised us that these security reports were reviewed, there was no documentation evidencing the specific reports reviewed, the dates of the reviews, the related findings and conclusions, and any subsequent investigative actions. Accordingly, assurance was lacking that erroneous or unauthorized activity, which could affect the integrity of DPSCS' data files, would be detected by management.

The State of Maryland's *Information Security Policy* requires that information systems generate audit records for all security-relevant events and that procedures must be developed to routinely (for example, daily or weekly) review audit records for indications of unusual activities, suspicious activities or suspected violations, and to report findings to appropriate officials for prompt resolution.

Recommendation 2

We recommend that ITCD

- a. log the use of all critical database system privileges and all direct modifications to significant data and security tables, and**
- b. document its review of all critical database and mainframe security software security reports and retain this documentation for future reference.**

Finding 3

The Department of Public Safety and Correctional Services (DPSCS) network was not properly secured.

Analysis

The DPSCS network was not properly secured.

- The primary firewalls installed to protect the DPSCS network from external untrusted entities allowed unnecessary and insecure connections to network devices in the internal network. The firewalls' rules were not configured to adequately secure connections into the network from networkMaryland and other untrusted sources. Therefore, critical network devices were susceptible

to attack which could result in a loss of data integrity or the interruption of critical network services. The State of Maryland's *Information Security Policy* requires that agency systems be configured to monitor and control communications at external boundaries. A similar condition was commented upon in our preceding audit report.

- Intrusion detection prevention system (IDPS) coverage did not exist for encrypted traffic from the Internet and other untrusted third parties entering the DPSCS network. Although the devices used to filter traffic and apply IDPS coverage to such traffic had the capability to decrypt and inspect such traffic for IDPS purposes, these features were not enabled on these devices. Additionally, host-based intrusion protection system software was not installed on any of the devices which received encrypted traffic. We identified 57 separate destination devices that received encrypted traffic. The *Information Security Policy* requires that agencies protect against malicious code and attacks by implementing protections including the use of IDPS to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

Recommendation 3

We recommend that ITCD

- a. configure its firewalls to achieve a “least privilege” security strategy giving individuals and devices only the access needed to perform necessary tasks (repeat);**
- b. perform a documented review and assessment of its network security risks from encrypted network traffic to its critical devices and identify how such traffic should be subject to IDPS; and**
- c. implement IDPS coverage as necessary, based on this review and assessment.**

Audit Scope, Objectives, and Methodology

We have audited of the Department of Public Safety and Correctional Services (DPSCS) – Information Technology and Communications Division (ITCD). Fieldwork associated with our audit of ITCD was conducted during the period from November 2014 to August 2015. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine ITCD's internal control over the DPSCS data center and network and to evaluate compliance with applicable State laws, rules, and regulations for the computer systems that support DPSCS and its user agencies.

In planning and conducting our audit, we focused on the major areas of operations based on assessments of significance and risk. The areas addressed by the audit included procedures and controls over the mainframe operating system, security software, and databases. Our audit also included an assessment of the security controls for critical routers, firewalls, switches, and virtual private network appliances, as well as an assessment of the security controls related to ITCD's use of anti-malware software to protect DPSCS' computers. We also determined the status of the findings included in our preceding audit report on ITCD.

ITCD's fiscal operations are audited separately as part of our audit of the DPSCS Office of the Secretary. The latest report on the Office of the Secretary was issued on November 18, 2015.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of ITCD's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. The reliability of data used in this report for background or informational purposes was not assessed.

ITCD's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records,

effectiveness and efficiency of operations, including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect ITCD's ability to operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to ITCD that did not warrant inclusion in this report.

The response from DPSCS, on behalf of ITCD, to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise DPSCS regarding the results of our review of its response.



APPENDIX

Department of Public Safety and Correctional Services

Office of the Secretary

300 E. JOPPA ROAD • SUITE 1000 • TOWSON, MARYLAND 21286-3020
(410) 339-5000 • FAX (410) 339-4240 • TOLL FREE (877) 379-8636 • V/TTY (800) 735-2258 • www.dpscs.maryland.gov

STATE OF MARYLAND

LARRY HOGAN
GOVERNOR

BOYD K. RUTHERFORD
LT. GOVERNOR

STEPHEN T. MOYER
SECRETARY

WILLIAM G. STEWART
DEPUTY SECRETARY
ADMINISTRATION

WAYNE A. WEBB
ACTING DEPUTY
SECRETARY OPERATIONS

RHEA L. HARRIS
ASSISTANT SECRETARY
PROGRAMS AND SERVICES

DAVID N. BEZANSON
ASSISTANT SECRETARY
CAPITAL PROGRAMS

December 15, 2015

Mr. Thomas J. Barnickel III, CPA
Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201

Dear Mr. Barnickel:

The Department of Public Safety and Correctional Services has reviewed the November 2015 Draft Audit Report of the Information Technology and Communications Division. We appreciate the constructive findings and recommendations that were made as the result of this audit.

Please find attached Chief Information Officer Kevin Combs' itemized responses to the Draft Audit Report findings and recommendations. Mr. Combs and his management team have begun, and will continue to implement corrective action to address the audit findings, and we will closely monitor their status in order to prevent any repeat audit findings in the next audit.

If you have any questions regarding this response, please contact me.

Sincerely,

Stephen T. Moyer
Secretary

Attachment

Copy: Roy McGrath, Deputy Chief of Staff, Governor's Office



Department of Public Safety and Correctional Services

Information Technology & Communications Division

Post Office Box 5743 • Pikesville, Maryland 21282-5743
Main №: 410-585-3100 • Facsimile №: 410-764-4035 • www.dpsscs.maryland.gov

December 15, 2015

STATE OF MARYLAND

LARRY HOGAN
GOVERNOR

BOYD K. RUTHERFORD
LT. GOVERNOR

STEPHEN T. MOYER
SECRETARY

WILLIAM G. STEWART
DEPUTY SECRETARY
ADMINISTRATION

WAYNE A. WEBB
ACTING DEPUTY
SECRETARY
OPERATIONS

RHEA L. HARRIS
ASSISTANT
SECRETARY
PROGRAMS AND
SERVICES

DAVID N. BEZANSON
ASSISTANT
SECRETARY
CAPITAL PROGRAMS

C. KEVIN COMBS
CHIEF INFORMATION
OFFICER

ARTHUR C. RAY, III
DEPUTY CHIEF
INFORMATION
OFFICER

Stephen T. Moyer, Secretary
Department of Public Safety and Correctional Services
300 East Joppa Road, Suite 1000
Towson, Maryland 21286-3020

Via William G. Stewart, Deputy Secretary for Administration
Department of Public Safety and Correctional Services
300 East Joppa Road, Suite 1000
Towson, Maryland 21286-3020

Dear Secretary Moyer:

The following is the Information Technology and Communications Division's (ITCD) response to the Legislative Audit regarding the Division's internal controls for the Department of Public Safety and Correctional Services (DPSCS) data center and network. ITCD will aggressively pursue implementation of the recommendations.

Network and Data Center Information Systems Security and Control

Finding 1

The Information Technology and Communications Division (ITCD) did not appropriately safeguard sensitive personally identifiable information.

Recommendation 1

We recommend that ITCD

- a. perform an inventory of its systems and identify all sensitive PII;**
- b. determine if it is necessary to retain this PII and delete all unnecessary PII;**
- c. determine if all necessary PII is properly protected by encryption or other substantial mitigating controls; and**
- d. use approved encryption methods to encrypt all sensitive PII not otherwise properly protected.**

We agree.

- a. An inventory of systems that contain PII was conducted prior to the audit and will continue on an ongoing basis. *Anticipated Completion: **Completed.***
- b. We have determined that it is necessary to retain the PII currently stored. *Anticipated Completion: **Completed.***

- c. We have determined that DPSCS databases do not require encryption because DPSCS has an acceptable level of security controls in place, such as Data Loss Prevention, Network Security Event Monitoring, and database change monitoring. Real time alerts are sent to the firewall team, and system log and access activation is reviewed weekly for unusual activity. The databases are housed in a secure location, firewalls rules and Access Control Lists (ACL) are in place, and databases that store PII have been identified in the Enterprise Architecture Resource (EAR). Individuals that have access to the data have fingerprint based background checks. Finally, data is transmitted through encrypted communication channels in compliance with DoIT and FBI CJIS security policies. *Anticipated Completion: **Completed.***
- d. PII data will be moved to an encrypted database or added software will be used to encrypt the existing fields for systems that need access to PII data. Encryption solutions are dependent on the Department's fiscal ability to acquire the needed software for encryption. *Anticipated Completion: **October 1, 2018***

Finding 2

Procedures for logging and monitoring critical database and mainframe security events were not sufficient.

Recommendation 2

We recommend that ITCD

- a. log the use of all critical database system privileges and all direct modifications to significant data and security tables; and**
- b. document its review of all critical database and mainframe security software security reports and retain this documentation for future reference.**

We agree.

- a. We will add to the current tables logged, and log all direct modifications to significant data and security tables. We anticipate that this may cause performance issues which we will document if changes need to be made affecting what is being logged. *Anticipated Completion: **July 1, 2016***
- b. A review process is now in place and will be conducted on a monthly basis. All reviews will be documented and retained for audit purposes. We will add additional information to the review process, as recommended. *Anticipated Completion: **Completed.***

Finding 3

The Department of Public Safety and Correctional Services (DPSCS) network was not properly secured.

Recommendation 3

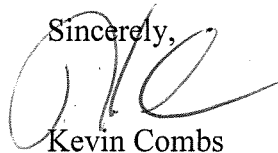
We recommend that ITCD

- a. configure its firewalls to achieve a “least privilege” security strategy giving individuals and devices only the access needed to perform necessary tasks (repeat);**
- b. perform a documented review and assessment of its network security risks from encrypted network traffic to its critical devices and identify how such traffic should be subject to the Intrusion Detection Prevention System (IDPS); and**
- c. implement IDPS coverage as necessary, based on this review and assessment.**

We agree.

- a. All items reported have been corrected. The copy of the rule sets provided to the auditors occurred while ITCD was making multiple changes related to various projects, system migrations, and system upgrades within the DPSCS environment. ITCD has changed its review process to better maintain the “least privilege” security posture. *Anticipated Completion: **Completed.***
- b. ITCD will change the current review process related to network security risks from encrypted network traffic to every six months. During the review, we will identify how such traffic should be subject to the IDPS. *Anticipated Completion: **October 1, 2016***
- c. ITCD will implement IDPS coverage, where necessary. *Anticipated Completion: **October 1, 2016***

Sincerely,



Kevin Combs

Chief Information Officer

cc: Steven F. Geppi, Director, Secretary's Office of Investigation, Intelligence
and Fugitive Apprehension
Christopher R. McCully, Director of Financial Services
Joseph M. Perry, Inspector General

AUDIT TEAM

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

R. Brendan Coffey, CPA, CISA
John C. Venturella, CISA
Information Systems Senior Auditors

Steven D. Bryant
Edward O. Kendall
Matthew D. Walbert
Information Systems Staff Auditors