

# Audit Report

---

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

September 2021

---



**OFFICE OF LEGISLATIVE AUDITS**  
DEPARTMENT OF LEGISLATIVE SERVICES  
MARYLAND GENERAL ASSEMBLY

### **Joint Audit and Evaluation Committee**

Senator Clarence K. Lam, M.D. (Senate Chair)	Delegate Carol L. Krimm (House Chair)
Senator Malcolm L. Augustine	Delegate Steven J. Arentz
Senator Adelaide C. Eckardt	Delegate Mark S. Chang
Senator George C. Edwards	Delegate Nicholas P. Charles II
Senator Katie Fry Hester	Delegate Andrea Fletcher Harrison
Senator Cheryl C. Kagan	Delegate Trent M. Kittleman
Senator Benjamin F. Kramer	Delegate David Moon
Senator Cory V. McCray	Delegate Julie Palakovich Carr
Senator Justin D. Ready	Delegate Geraldine Valentino-Smith
Senator Craig J. Zucker	One Vacancy

### **To Obtain Further Information**

Office of Legislative Audits  
301 West Preston Street, Room 1202  
Baltimore, Maryland 21201  
Phone: 410-946-5900 · 301-970-5900 · 1-877-486-9964 (Toll Free in Maryland)  
Maryland Relay: 711  
TTY: 410-946-5401 · 301-970-5401  
E-mail: [OLASWebmaster@ola.state.md.us](mailto:OLASWebmaster@ola.state.md.us)  
Website: [www.ola.state.md.us](http://www.ola.state.md.us)

### **To Report Fraud**

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.

### **Nondiscrimination Statement**

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 United States Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.



Victoria L. Gruber  
Executive Director

DEPARTMENT OF LEGISLATIVE SERVICES  
OFFICE OF LEGISLATIVE AUDITS  
MARYLAND GENERAL ASSEMBLY

Gregory A. Hook, CPA  
Legislative Auditor

September 10, 2021

Senator Clarence K. Lam, M.D., Senate Chair, Joint Audit and Evaluation Committee  
Delegate Carol L. Krimm, House Chair, Joint Audit and Evaluation Committee  
Members of Joint Audit and Evaluation 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 provider for DPSCS.

Our audit disclosed that sensitive personally identifiable information maintained by ITCD was stored without adequate safeguards. In addition, intrusion detection prevention system coverage did not exist for certain untrusted encrypted traffic entering the DPSCS network.

Our audit included a review to determine the status of five findings that were contained in certain preceding audit reports. Specifically, our audit included a review to determine the status of the three findings contained in our preceding audit report on DPSCS – ITCD, dated January 6, 2016 and two findings from our DPSCS – Office of the Secretary and Other Units audit report, dated November 18, 2015. We determined that ITCD satisfactorily addressed four of these findings. The remaining finding is repeated in this report.

DPSCS' response to this report, on behalf of ITCD, is included as an appendix to this report. We reviewed the response to our findings and recommendations and have concluded that the corrective actions identified are sufficient to address all issues. However, we remain concerned that the corrective actions indicated to

provide adequate safeguards over personally identifiable information will take an extended period to implement. As a result, as noted in an Auditor Comment inserted in the DPSCS response, we believe there is a need to implement compensating controls in the interim to provide appropriate safeguards. Additionally, we have edited DPSCS' response to remove certain detailed information regarding information systems security, as allowed by our policy.

We wish to acknowledge the cooperation extended to us during the audit by ITCD. We also wish to acknowledge DPSCS' and ITCD's willingness to address the audit issues and implement appropriate corrective actions.

Respectfully submitted,

A handwritten signature in black ink that reads "Gregory A. Hook". The signature is written in a cursive style with a large, stylized 'G' and 'H'.

Gregory A. Hook, CPA  
Legislative Auditor

## **Background Information**

### **Agency Responsibilities and Financial Activity**

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. ITCD provides data, information, and communications services to DPSCS, criminal justice entities, and the public. In addition, ITCD maintains numerous application systems containing sensitive information.

Furthermore, ITCD operates a wide area network (WAN) that connects with many 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. According to the State's records, ITCD's fiscal year 2020 expenditures totaled \$42 million.

Our audit focused exclusively on ITCD computer and network operations. An audit of ITCD fiscal operations was conducted as part of the audit of DPSCS – Central Operations, and a separate report was issued on November 20, 2019.

### **Status of Findings From Preceding Audit Reports**

Our audit included a review to determine the status of the three findings contained in our preceding audit report on DPSCS – ITCD, dated January 6, 2016 and two findings from our DPSCS – Office of the Secretary and Other Units audit report, dated November 18, 2015.

As disclosed in Figure 1 on page 4, we determined that four of the five findings were satisfactorily addressed. The remaining finding is repeated in this report.

**Figure 1**  
**Status of Preceding Findings**

<b>Preceding Finding</b>	<b>Finding Description</b>	<b>Implementation Status</b>
<b>DPSCS – ITCD</b> <b>Audit Report dated January 6, 2016</b>		
Finding 1	Personally identifiable information was not appropriately safeguarded.	<b>Repeated</b> (Current Finding 1)
Finding 2	Procedures for logging and monitoring critical database and mainframe security events were not sufficient.	Not repeated
Finding 3	The DPSCS network was not properly secured.	Not repeated
<b>DPSCS – Office of the Secretary and Other Units</b> <b>Audit Report dated November 18, 2015</b>		
Finding 5	Personally identifiable information was not appropriately safeguarded.	Not repeated
Finding 6	Account, password, and monitoring controls were not sufficient.	Not repeated

## Findings and Recommendations

### Sensitive Personally Identifiable Information (PII)

**Finding 1**  
**ITCD maintained sensitive PII in a manner that did not provide adequate safeguards.**

#### Analysis

ITCD maintained sensitive PII in a manner that did not provide adequate safeguards. ITCD supported computer operations for multiple mainframe applications and a server application, which processed such sensitive information, but without adequate safeguards. As of March 2020, we noted that four of these applications' databases included a significant number of unique sensitive information records which were maintained in a manner that made the information vulnerable to improper disclosure. ITCD personnel advised us that this sensitive PII was not subject to other substantial mitigating controls. Similar conditions were commented upon in our preceding audit report.

Detailed aspects of this finding were omitted from this report; however, the related detailed information, including a sensitive information record count, was previously shared with ITCD for purposes of implementing the following recommendations.

The State of Maryland *Information Technology Security Manual* requires that agencies protect confidential data using adequate safeguards and/or other substantial mitigating controls.

#### **Recommendation 1**

**We recommend that ITCD implement appropriate information security safeguards for the sensitive PII it maintains (repeat).**

### **Network Security**

#### **Finding 2**

**Intrusion detection prevention system coverage did not exist for certain untrusted encrypted traffic.**

#### **Analysis**

Intrusion detection prevention system (IDPS) coverage did not exist for certain untrusted encrypted traffic entering the DPSCS network. ITCD operated a network appliance having integrated IDPS. Although the network-based IDPS used by ITCD had the capability to decrypt and analyze encrypted network traffic received, this feature was not enabled for a significant portion of such traffic. Additionally, server host-based intrusion prevention system coverage was not used for this untrusted encrypted traffic. We identified 11 firewall rules that allowed encrypted traffic from any source to 27 unique network destinations within DPSCS' internal network without IDPS coverage.

The aforementioned absence of IDPS coverage creates network security risk as the untrusted encrypted traffic could contain undetected malicious data. The State of Maryland *Information Technology Security Manual* requires protection against malicious code and attacks by using IDPS to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

#### **Recommendation 2**

**We recommend that ITCD perform a documented review and assessment of its network security risks and identify how IDPS coverage should be applied**

**to its network for all untrusted traffic, including encrypted traffic, and implement this coverage.**

## **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 February 2020 to September 2020. 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 the 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 its 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 security procedures and controls over the mainframe operating system, security software, and critical 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 wireless connectivity. We also determined the status of the three findings contained in our preceding audit report on ITCD as well as the status of two findings included in our audit report of DPSCS – Office of the Secretary and Other Units dated November 18, 2015.

ITCD's fiscal operations are audited separately as part of our audit of DPSCS – Central Operations. The most recent report on DPSCS – Central Operations was issued on November 20, 2019.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and to the extent practicable, observations of ITCD operations. We also performed other auditing procedures that we considered necessary to achieve our audit 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. As provided in *Government Auditing Standards*, there are five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Each of the five components, when significant to the audit objectives, and as applicable to ITCD, were considered by us during the course of this audit.

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 a 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. Aspects of certain findings contained in this report address issues of a sensitive nature, and we have omitted that detailed information from this report. However, for the purposes of implementing the related recommendations that information was previously shared with ITCD.

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

6852 4<sup>th</sup> Street, Sykesville, Maryland 21784  
(410) 339-5000 • [www.dpscs.maryland.gov](http://www.dpscs.maryland.gov)

STATE OF MARYLAND

LARRY HOGAN  
GOVERNOR

BOYD K. RUTHERFORD  
LT. GOVERNOR

ROBERT L. GREEN  
SECRETARY

RACHEL SESSA  
CHIEF OF STAFF

CHRISTOPHER McCULLY  
DEPUTY SECRETARY  
ADMINISTRATION

WAYNE HILL  
DEPUTY SECRETARY  
OPERATIONS

CAROLYN J. SCRUGGS  
ASSISTANT SECRETARY

GARY W. McLHINNEY  
ASSISTANT SECRETARY

August 27, 2021

Mr. Gregory A. Hook, CPA  
Legislative Auditor  
Department of Legislative Services  
Office of Legislative Audits  
301 West Preston Street, Room 1202  
Baltimore, Maryland 21201

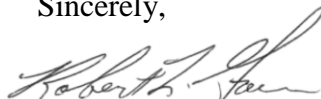
Dear Mr. Hook:

The Department of Public Safety and Correctional Services (DPSCS) has reviewed the Draft Audit Report dated August 11, 2021 for the DPSCS – 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 Stanley Lofton's itemized responses to the findings and recommendations. Corrective action has or will be taken for the findings noted by the Legislative Auditor, and we will closely monitor their reported 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,

  
Robert L. Green  
Secretary

Attachment

Cc: Walter Pete Landon, Deputy Chief of Staff

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

**Agency Response Form**

**Sensitive Personally Identifiable Information (PII)**

**Finding 1**  
**ITCD maintained sensitive PII in a manner that did not provide adequate safeguards.**

**We recommend that ITCD implement appropriate information security safeguards for the sensitive PII it maintains (repeat).**

<b>Agency Response</b>			
<b>Analysis</b>			
<b>Please provide additional comments as deemed necessary.</b>			
<b>Recommendation 1</b>	<b>Agree</b>	<b>Estimated Completion Date:</b>	<b>12/31/2025</b>
<b>Please provide details of corrective action or explain disagreement.</b>	<p><b>By March 2022, the Department's distributed servers will be corrected to provide adequate protection of the PII data.</b></p> <p><b>The Department will also implement new systems to provide adequate protection for the PII data now associated to mainframe systems. This will include:</b></p> <ul style="list-style-type: none"><li><b>a. Submitting a grant application for funds to implement a fully web based restitution module by 12/31/22. While it is the Department's desire to implement this by 12/31/22, this may not occur until sometime in 2023, depending on funding; and</b></li><li><b>b. Awarding a project to implement a fully web based criminal history system. This project, once awarded, is estimated to take four years to implement, and will provide sufficient safeguards of PII data. The Department expects to award the contract for this system by the end of November 2021, and it should be in operation by 12/31/2025.</b></li></ul>		

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

**Agency Response Form**

**Auditor's Comment:** ITCD's response addressed the safeguarding of PII across both server-based and mainframe systems. We are concerned that ITCD's resolution timeline goes far out into the future for both systems (December 2022 and December 2025, respectively). Since the timing of this resolution is based on replacing the respective systems, the delay is understandable. However, we remain concerned that until the system replacements are accomplished, the PII security risk, part of which was also cited in the prior audit, will continue for projected long periods without adequate safeguards in place. Accordingly, during the system replacement periods, ITCD needs to take prompt action to implement other substantial mitigating controls, to the extent possible, as required by the State of Maryland *Information Technology Security Manual*. We discussed the need to implement this compensating controls approach during the audit exit meeting. This approach would require ITCD to consistently implement three mitigating controls, which involve performing data loss prevention, network security event monitoring, and strict database change monitoring. We believe that ITCD has adequate tools and personnel necessary to support most of those controls, but may require additional assets to achieve appropriate data loss prevention control.

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

**Agency Response Form**

**Network Security**

**Finding 2**

**Intrusion detection prevention system coverage did not exist for certain untrusted encrypted traffic.**

**We recommend that ITCD perform a documented review and assessment of its network security risks and identify how IDPS coverage should be applied to its network for all untrusted traffic, including encrypted traffic, and implement this coverage.**

<b>Agency Response</b>			
<b>Analysis</b>			
<b>Please provide additional comments as deemed necessary.</b>			
<b>Recommendation 2</b>	<b>Agree</b>	<b>Estimated Completion Date:</b>	<b>12/31/2021</b>
<b>Please provide details of corrective action or explain disagreement.</b>	<b>DPSCS will perform a documented quarterly review and assessment of its network security risks relative to IDPS coverage. Additionally, we will identify how network IDPS coverage (including coverage for encrypted traffic) should be best applied to its network, and subsequently implement IDPS coverage for all critical portions of its network, which were assessed as needing such coverage.</b>		

AUDIT TEAM

**R. Brendan Coffey, CPA, CISA**

**Edwin L. Paul, CPA, CISA**

Information Systems Audit Managers

**Edward O. Kendall, CISA**

**Matthew D. Walbert, CISA**

Information Systems Senior Auditors

**Dominick R. Abril**

**Charles O. Price**

Information Systems Staff Auditors