Audit Report

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

October 2025

Public Notice

In compliance with the requirements of the State Government Article Section 2-1224(i), of the Annotated Code of Maryland, the Office of Legislative Audits has redacted cybersecurity findings and related auditee responses from this public report.

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

To Obtain Further Information

Office of Legislative Audits
The Warehouse at Camden Yards
351 West Camden Street, Suite 400
Baltimore, Maryland 21201
Phone: 410-946-5900
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: webmaster@ola.maryland.gov
Website: ola.maryland.gov

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

Brian S. Tanen, CPA, CFE
Legislative Auditor

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

October 1, 2025

Senator Shelly L. Hettleman, Senate Chair, Joint Audit and Evaluation Committee
Delegate Jared Solomon, 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). The ITCD operates the DPSCS data center with an associated wide area network and maintains application systems which provide computing resources for DPSCS operating agencies. 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. Our audit did not include ITCD's fiscal operations which are audited separately by us and are reported upon in an audit report under the name of DPSCS - Central Operations.

Our audit disclosed certain cybersecurity-related findings. However, in accordance with the State Government Article, Section 2-1224(i) of the Annotated Code of Maryland, we have redacted the findings from this audit report. Specifically, State law requires the Office of Legislative Audits to redact cybersecurity findings in a manner consistent with auditing best practices before the report is made available to the public. The term "cybersecurity" is defined in the State Finance and Procurement Article, Section 3.5-301(b), and using our professional judgment we have determined that the redacted findings fall under the referenced definition. The specifics of the cybersecurity findings were previously communicated to those parties responsible for acting on our recommendations.

DPSCS' response to this audit, on behalf of ITCD, is included as an appendix to this report. Consistent with State law, we have redacted the elements of DPSCS' response related to the cybersecurity audit findings. We reviewed the response to our findings and related recommendations, and have concluded that the corrective actions identified are sufficient to address all issues.

We wish to acknowledge the cooperation extended to us during the audit by ITCD.

Respectfully submitted,

Brian S. Tanen

Brian S. Tanen, CPA, CFE
Legislative Auditor

Table of Contents

Background Information

Agency Responsibilities

The Department of Public Safety and Correctional Services' (DPSCS) Information Technology and Communications Division (ITCD) 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.

The ITCD also operates a wide area network connected to many statewide sites, such as local law enforcement agencies, and the DPSCS data center's local network providing access to various information technology services including mainframe computer-based applications (for example, the Criminal Justice Information System), database management, network services, and the internet. According to the agency's records, ITCD's fiscal year 2025 expenditures totaled approximately $61.9 million. Expenditures have significantly increased during the audit period (from $42 million in fiscal year 2020) primarily due to an increase in employee positions and equipment upgrades.

We conduct separate audits of DPSCS Central Operations (which includes the Division of Parole and Probation), DPSCS Regional Operations, and Maryland Correctional Enterprises. This audit focused exclusively on the ITCD computer and network operations. Certain ITCD fiscal and operational activities are subject to audit during the DPSCS Central Operations audit.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the two findings contained in our preceding audit report dated September 2021. See Figure 1 for the results of our review.

Figure 1 Status of Preceding Findings		
Preceding Finding	**Finding Description**	**Implementation Status**
Finding 1	Redacted cybersecurity-related finding.[1]	Status Redacted[1]
Finding 2	Redacted cybersecurity-related finding.[1]	Status Redacted[1]

[1] The finding description as well as the implementation status of this cybersecurity-related finding has been redacted for the publicly available report in accordance with State Government Article, Section 2-1224(i) of the Annotated Code of Maryland.

Findings and Recommendations

Information Technology

We determined that the Information Technology section, including Findings 1 through 3 related to "cybersecurity," as defined by the State Finance and Procurement Article, Section 3.5-301(b) of the Annotated Code of Maryland, and therefore are subject to redaction from the publicly available audit report in accordance with the State Government Article 2-1224(i). Consequently, the specifics of the following findings, including the analysis, related recommendations, along with DPSCS' responses, have been redacted from this report copy.

Finding 1
Redacted cybersecurity-related finding.

Finding 2
Redacted cybersecurity-related finding.

Finding 3
Redacted cybersecurity-related finding.

Audit Scope, Objectives, and Methodology

We have audited 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 2024 to July 2025. 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 controls 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. A description of the specific information systems and related control functions addressed by the audit have been redacted from this report as required by State Government Article Section 2-1224(i) described below. We also determined the status of the findings contained in our preceding audit report on ITCD.

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 September 17, 2024.

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. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk, the timing or dollar amount of the transaction, or the significance of the transaction to the area of operation reviewed. As a matter of course, we do not normally use sampling in our tests, so unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, unless sampling is specifically indicated in a finding, the results from any tests conducted or disclosed by us cannot be used to project those results to the entire population from which the test items were selected.

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 (including information systems resources); 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 significant deficiencies in the design or operation of internal control that could adversely affect ITCD's ability to operate information systems resources 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.

State Government Article Section 2-1224(i) requires that we redact in a manner consistent with auditing best practices any cybersecurity findings before a report is made available to the public. This results in the issuance of two different versions of an audit report that contains cybersecurity findings – a redacted version for the public and an unredacted version for government officials responsible for acting on our audit recommendations.

The State Finance and Procurement Article, Section 3.5-301(b), states that cybersecurity is defined as "processes or capabilities wherein systems, communications, and information are protected and defended against damage, unauthorized use or modification, and exploitation". Based on that definition, and in our professional judgement, we concluded that all findings in this report fall under that definition. Consequently, for the publicly available audit report all specifics as to the nature of cybersecurity findings and required corrective actions have been redacted. We have determined that such aforementioned practices, and government auditing standards, support the redaction of this information from the public audit report. The specifics of these cybersecurity findings have been communicated to ITCD and those parties responsible for acting on our recommendations in an unredacted audit report.

The response from DPSCS, on behalf of ITCD, to our findings and recommendations is included as an appendix to this report. Depending on the version of the audit report, responses to any cybersecurity findings may be redacted in accordance with State law. 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

6776 Reisterstown Road, Baltimore, Maryland 21215
410-585-3346 – TOLL FREE 877-379-8636 • www.dpscs.maryland.gov

September 30, 2025

Mr. Brian S. Tanen, CPA, CFE
Legislative Auditor
Office of Legislative Audits
The Warehouse at Camden Yards
351 West Camden Street, Suite 400
Baltimore, MD 21201

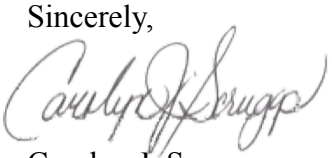
Dear Mr. Tanen,

The Department of Public Safety and Correctional Services (DPSCS) has reviewed the Office of Legislative Audits Draft Audit Report dated September 2025 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 corrective action 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,



Carolyn J. Scruggs
Secretary

Attachment

Copy: Adam Flasch, Deputy Chief of Staff for Public Safety and Homeland Security

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

Agency Response Form

Information Technology

The Office of Legislative Audits (OLA) has determined that the Information Technology section, including Findings 1 through 3 related to "cybersecurity," as defined by the State Finance and Procurement Article, Section 3.5-301(b) of the Annotated Code of Maryland, and therefore are subject to redaction from the publicly available audit report in accordance with the State Government Article 2-1224(i). Although the specifics of the following findings, including the analysis, related recommendations, along with DPSCS' responses, have been redacted from this report copy, DPSCS' responses indicated agreement with the findings and related recommendations.

Finding 1
Redacted cybersecurity-related finding.

Agency Response has been redacted by OLA.

Finding 2
Redacted cybersecurity-related finding.

Agency Response has been redacted by OLA.

Finding 3
Redacted cybersecurity-related finding.

Agency Response has been redacted by OLA.

AUDIT TEAM

R. Brendan Coffey, CPA, CISA
Edwin L. Paul, CPA, CISA
Michael K. Bliss, CISA
Information Systems Audit Managers

Eric Alexander, CPA, CISA
Charles O. Price
Information Systems Senior Auditors

Christopher C. Pitre
Neha S. Tirkey
Information Systems Staff Auditors