Audit Report

Judiciary
Judicial Information Systems

August 2021

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

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: OLAWebmaster@ola.state.md.us
Website: 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.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

August 23, 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 Judiciary – Judicial Information Systems (JIS). Our audit included an internal control review of the Judiciary's data center and the network administered by JIS. JIS provides computing and network resources and operates as a computer services provider for the Judiciary.

Our audit disclosed that JIS did not have sufficient controls over authenticating remote network connections.

Our audit included a review to determine the status of five findings that were contained in the preceding audit report. I would like to call your attention to our determination that JIS satisfactorily addressed all five of these findings.

The Judiciary's response to this report, on behalf of JIS, is included as an appendix to this report. We reviewed the response to our finding and related recommendation, and have concluded that the corrective actions identified are sufficient to address all issues.

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900 · Toll Free in Maryland 877-486-9964
Fraud Hotline 877-FRAUD-11 · www.ola.state.md.us

We wish to acknowledge the cooperation extended to us during the audit by JIS. We also wish to acknowledge the Judiciary's and JIS' willingness to address the audit issue and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook, CPA
Legislative Auditor

Background Information

Agency Responsibilities

The Judiciary operates the Judicial Information Systems (JIS) on behalf of the State court systems. JIS develops and maintains State court system applications, operates a statewide computer network, and is responsible for data center contingency planning. JIS' fiscal year 2020 expenditures totaled approximately $61.4 million, according to State records.

JIS maintains two data centers and supports all major information technology initiatives in the District Courts, the Circuit Courts, the Appellate Courts, as well as other court-related offices. The Judiciary is transitioning courts across the state onto the Maryland Electronic Courts (MDEC) system that supports case initiation, scheduling, disposition, and other record keeping. As of June 28, 2021, 21 of 24 jurisdictions have been converted to MDEC.

JIS operates a computer wide area network (WAN) that connects to all units of the Maryland State Judiciary including the Administrative Office of the Courts, the District Courts, and the Circuit Courts. The WAN connects the remote court locations to the MDEC and other JIS maintained applications. Furthermore, numerous local area networks, across all remote court locations, can access external agencies through networkMaryland as well as the internet.

Our audit focused exclusively on the computer and network operations of the JIS data centers. An audit of JIS fiscal operations was conducted as part of the audit of the Judiciary, and a separate report was issued on April 7, 2021.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the five findings contained in our preceding audit report dated August 18, 2016. We determined that JIS satisfactorily addressed these findings.

Findings and Recommendations

Finding 1
Remote access to the internal Judicial Information Systems (JIS) network by employees, courts-affiliated personnel, and authorized contractors used a single authentication measure rather than the more secure multi-factor authentication.

Analysis
We determined that the remote access by employees, courts-affiliated personnel, and authorized contractors to JIS' internal network, using a Virtual Private Network (VPN) connection, required a stronger security authentication measure than was in place during the audit. Our review noted that 5,139 user accounts across the above user categories had such VPN-based remote network access.

These remote VPN connections into JIS' internal network did not require multi-factor authentication (MFA) for establishing access. Instead, access was provided based upon only single factor authentication. MFA uses two or more different credential factors to authenticate user network connections. Access to critical networks and resources requires layers of security protections which include use of MFA, to help prevent security risks tied to compromised user credentials.

Best practices, as specified in the State of Maryland *Information Technology Security Manual*, require Maryland agencies[1] to ensure that MFA mechanisms are employed for all remote access to networks.

Recommendation 1
We recommend that JIS implement multi-factor authentication for remote connections into the JIS network by employees, courts-affiliated personnel, and authorized contractors.

Audit Scope, Objectives, and Methodology

We have audited the Judiciary – Judicial information Systems (JIS). Fieldwork associated with our audit of JIS was conducted during the period from August 2020 to December 2020. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan

[1] As an independent branch of State government, the *Manual's* requirements do not apply to the Judiciary and JIS.

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 JIS' internal control over its data centers and network and to evaluate its compliance with applicable State laws, rules, and regulations for the computer systems that support the State courts and related agencies of the Judiciary.

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 databases. Our audit also included an assessment of the security controls for the network infrastructure and critical network devices (for example firewalls), and JIS' use of malware protection software to protect JIS' computers. We also determined the status of the findings contained in our preceding audit report on JIS.

JIS' fiscal operations are audited separately as part of our audit of the Judiciary. The most recent fiscal compliance audit that covered the Judiciary's fiscal operations was issued on April 7, 2021.

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 JIS 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.

JIS' 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 JIS, 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 a finding relating to a condition that we consider to be a significant deficiency in the design or operation of internal control that could adversely affect JIS' ability to operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our audit did not disclose any instance of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to JIS that did not warrant inclusion in this report.

The response from the Judiciary, on behalf of JIS, 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 JIS regarding the results of our review of its response.

APPENDIX

Court of Appeals of Maryland
Robert C. Murphy Courts of Appeal Building
361 Rowe Boulevard
Annapolis, Maryland 21401-1699

MARY ELLEN BARBERA
Chief Judge

August 19, 2021

Mr. Gregory A. Hook, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Hook:

We have received the Maryland Office of Legislative Audit's draft audit report pertaining to the Judiciary's Judicial Information Systems (JIS), dated August 2021. The attached document contains our response to the finding and recommendation in the audit report.

We believe we have responded in full to the finding and recommendation.

Sincerely,

Mary Ellen Barbera
Chief Judge of the Court of Appeals

Pamela Q. Harris
State Court Administrator

Judiciary
Judicial Information Systems

Agency Response Form

Finding 1
Remote access to the internal Judicial Information Systems (JIS) network by employees, courts-affiliated personnel, and authorized contractors used a single authentication measure rather than the more secure multi-factor authentication.

We recommend that JIS implement multi-factor authentication for remote connections into the JIS network by employees, courts-affiliated personnel, and authorized contractors.

Agency Response			
Analysis			
Please provide additional comments as deemed necessary.			
Recommendation 1	Agree	**Completion Date:**	June 23, 2021
Please provide details of corrective action or explain disagreement.	Judicial Information Systems (JIS) recognizes the importance of authentication techniques that help prevent against account breaches and, as such, takes the necessary actions to further secure the Judiciary's network operations. In June 2019, JIS implemented multi-factor authentication (MFA) for system administrators who use remote access technology to connect to the Judiciary's network. Further to this, JIS began internal testing of MFA for use by all individuals who use remote access technologies to access the Judiciary's network. Following careful consideration, JIS began pilot testing MFA with several user groups. Due to the pandemic and its attendant issues, the timing for implementation of MFA required contemplation of the impact to court business operations. As such, the decision was made to hold the implementation of MFA for all individuals who use remote access technologies until the Judiciary resumed full operations on April 26, 2021. MFA was fully implemented for all Judiciary users of a predominate operating system who connect to the Judiciary network using remote access technology on June 23, 2021.		

AUDIT TEAM

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

Michael K. Bliss
Matthew D. Walbert, CISA
Information Systems Senior Auditors

Dominick R. Abril
Vickey K. Micah
Charles O. Price
Malcolm J. Woodard
Information Systems Staff Auditors