

Audit Report

---

**Judiciary**  
**Judicial Information Systems**

August 2016

---



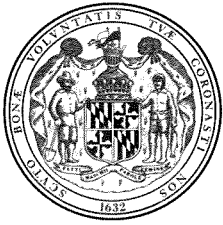
**OFFICE OF LEGISLATIVE AUDITS**  
**DEPARTMENT OF LEGISLATIVE SERVICES**  
**MARYLAND GENERAL ASSEMBLY**

**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](mailto:OLAWebmaster@ola.state.md.us)  
Website: [www.ola.state.md.us](http://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

August 18, 2016

Thomas J. Barnickel III, CPA  
Legislative Auditor

Senator Guy J. Guzzone, Co-Chair, Joint Audit Committee  
Delegate C. William Frick, Co-Chair, Joint Audit Committee  
Members of Joint Audit Committee  
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the Judicial Information Systems (JIS) of the Judiciary. Our audit included an internal control review of the JIS data center and the network administered by JIS that supports the Judiciary and the Courts of Maryland. JIS provides computing and network resources and operates as a computer services bureau for the Judiciary.

Our audit disclosed that appropriate safeguards were not established to protect sensitive information, such as social security numbers, names, and dates of birth, maintained in a critical circuit court database. In addition, the JIS network was not adequately secured against external threats because the firewalls used to protect the network were not properly configured or monitored. Furthermore, the intrusion detection prevention system coverage for the network was not effectively deployed. For example, encrypted traffic entering the network was not being analyzed for malicious activity. Finally, malware protection software used to protect JIS devices was not installed on many servers and workstations, and certain contractors had unnecessary network-level access to critical JIS computers.

The Judiciary's response to this audit, on behalf of JIS, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the audit by JIS.

Respectfully submitted,

Thomas J. Barnickel III, CPA  
Legislative Auditor



## **Table of Contents**

<b>Background Information</b>	<b>4</b>
Agency Responsibilities	4
Status of Findings From Preceding Audit Report	4
<b>Findings and Recommendations</b>	<b>5</b>
<b>Network and Data Center Information Systems Security and Control</b>	
Finding 1 – The Judicial Information Systems (JIS) maintained a circuit court database which contained 150,454 unique social security numbers with names and (in some cases) dates of birth without adequate safeguards.	5
* Finding 2 – Network devices, used to help protect the JIS network, were not configured to adequately secure connections from untrusted sources and were not properly monitored, and password controls did not properly protect the perimeter firewalls.	6
Finding 3 – Intrusion detection prevention system (IDPS) coverage for the network was not effectively deployed. In addition, updates to the IDPS device and backups of the device configuration were not properly performed, and administrative access to the device was not properly restricted.	7
Finding 4 – JIS had not installed malware protection software on 151 servers and also lacked assurance that malware protection software was installed on all of its workstations.	9
Finding 5 – Numerous contractors had unnecessary network-level access to critical JIS computers and 42 publicly accessible servers were located in the internal JIS network thereby exposing other computers in the internal network to increased risk of attack.	9
<b>Audit Scope, Objectives, and Methodology</b>	<b>11</b>
<b>Agency Response</b>	<b>Appendix</b>

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

## **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. According to the State's records, the JIS fiscal year 2015 expenditures totaled approximately \$47.1 million.

JIS operates a mainframe computer for court applications (such as, district court case management) and a server that supports the Traffic Processing Center (traffic citations). In addition, there are six servers that support the Uniform Court System (UCS), which provides court case management to 22 Circuit Courts. The UCS supports case initiation, scheduling, disposition, expungement, and other record keeping. JIS primarily serves three groups of users: public customers, Judicial Data Center personnel, and remote Court users. JIS also supplies traffic case dispositions and court case data processed by JIS to computer systems maintained by the Motor Vehicle Administration and the Department of Public Safety and Correctional Services, respectively.

JIS also has a Wide Area Network (WAN) which operates on an infrastructure owned and supported by a communications service provider. This WAN connects users to the various component units of the Judiciary including the Administrative Office of the Courts, the District Courts, and the Circuit Courts. The WAN is also used to connect the remote court locations to the UCS. JIS staff connects to the WAN to maintain the regional UCS servers and update the application software. Additionally, the WAN is used for remote connectivity from court offices to JIS mainframe applications. Furthermore, numerous local area networks, across all remote court locations, can access the UCS and can access external agencies through the Internet and networkMaryland.

Our audit focused exclusively on the computer and network operations of the JIS data center. An audit of the JIS fiscal operations was conducted as part of the audit of the Judiciary, and a separate report was issued on July 16, 2013.

### **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 February 28, 2012. We determined that JIS 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 Judicial Information Systems (JIS) maintained a circuit court database which contained 150,454 unique social security numbers with names and (in some cases) dates of birth without adequate safeguards.**

#### **Analysis**

JIS inappropriately stored sensitive personally identifiable information (PII) in clear text. Specifically, as of February 5, 2016, we identified a critical circuit court database containing 150,454 unique social security numbers along with names and (in some cases) dates of birth that were not encrypted. In addition, we determined that this sensitive PII was not protected by other substantial mitigating controls.

This PII, which is commonly associated with identity theft, should be protected by appropriate information system security controls. According to industry best practices, as described by the State of Maryland *Information Security Policy*, agencies should protect confidential data using encryption technologies and/or other substantial mitigating controls.

#### **Recommendation 1**

**We recommend that JIS**

- 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**

**Network devices, used to help protect the JIS network, were not configured to adequately secure connections from untrusted sources and were not properly monitored, and password controls did not properly protect the perimeter firewalls.**

### **Analysis**

The network devices used to help secure the JIS network were not properly configured, and monitored, and password controls did not properly protect the perimeter firewalls.

- The network devices installed to protect the JIS network allowed unnecessary and insecure connections to the internal network. Specifically, the perimeter firewalls' rules were not configured to adequately secure connections into the network from the Internet, networkMaryland, and other untrusted sources, and a critical router allowed unnecessary access to the JIS network from several untrusted sources. In addition, many outdated rules existed on these firewalls. Therefore, critical network devices were susceptible to attack which could result in a loss of data integrity or the interruption of essential network services. The Administrative Office of the Courts Judicial Information Systems' *Information Security Policy* states that information systems should be configured to monitor and control communications at the external boundaries of the information systems and at key internal boundaries within the systems. Similar conditions were commented upon in our preceding audit report.
- The perimeter firewalls were not configured to send email alerts to firewall administrators related to firewall problems and possible attacks on the firewalls. In addition, firewall logs, which log a variety of network events and sensitive actions as they occur, were not reviewed.
- Password controls did not ensure that the perimeter firewalls were properly protected. Specifically, password controls over access to these firewalls did not meet any of the State of Maryland *Information Security Policy* password requirement best practices. For example, the minimum password length was three characters and password complexity was not enforced.

### **Recommendation 2**

**We recommend that JIS**

- a. configure its firewalls and routers to achieve a "least privilege" security strategy giving individuals, entities, and devices only those network access privileges needed to perform assigned tasks (repeat);**



- b. **configure the firewalls to send automatic email alerts to administrators concerning high severity firewall operational events;**
- c. **regularly review the firewalls' logs using automated tools, and investigate unusual and suspicious items, with such reviews and investigations being documented and retained for future reference; and**
- d. **enable the firewalls' available password control settings to meet the requirements of the State's *Information Security Policy*.**

### **Finding 3**

**Intrusion detection prevention system (IDPS) coverage for the network was not effectively deployed. In addition, updates to the IDPS device and backups of the device configuration were not adequately performed or controlled, and administrative access to the device was not properly restricted.**

### **Analysis**

IDPS coverage for the JIS network was configured to detect, but not block malicious traffic, and was not used to analyze encrypted traffic entering the network. Additionally, updates and backups to the IDPS device were not adequately performed or controlled and administrative access to the device was not properly restricted. Consequently, the network was highly susceptible to malicious activity.

- The IDPS device was not configured to block malicious traffic intrusion attempts identified by the device but rather was configured only to detect and report suspected malicious traffic. In addition, at the time of our review in January 2016, we found JIS had discontinued IDPS log reviews effective February 2015 and only reviewed two IDPS daily summary reports. However, these two reports did not contain detailed information and could not be used to investigate potential network intrusions identified by the IDPS device.
- IDPS coverage did not exist for encrypted traffic entering the JIS network. We were advised by JIS personnel that host-based intrusion protection systems (HIPS) were not in use on JIS servers that processed encrypted traffic, and encrypted traffic was not decrypted for inspection by the JIS network-based IDPS. The absence of IDPS coverage for such encrypted traffic creates network security risk as such traffic could contain malicious data which would not be detected or blocked. Complete IDPS coverage includes the use of a properly-configured, network-based IDPS that decrypts and analyzes encrypted traffic, and/or the effective use of a HIPS on critical

servers, to aid significantly in the detection and prevention of, and response to, potential network security breaches and attacks.

- Updates to the IDPS device and backups of the device configuration were not being performed, and administrative access to the device was not properly restricted. Specifically, as of January 2016, IDPS signatures (used to detect malicious traffic) had not been updated on the IDPS device for over 12 months because the device license expired on January 1, 2015. In addition, as of January 2016, the device configuration files had not been backed up since January 15, 2013. Finally, administrative access to the device was not restricted to originate from only authorized sources.

Strong network security uses a layered approach, relying on various resources structured according to assessed network security risks. A properly configured IDPS can aid significantly in the detection/prevention of and response to potential network security breaches and attacks. Also, the Administrative Office of the Courts Judicial Information Systems' *Information Security Policy* states that the Judiciary will 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 JIS**

- a. perform a documented review and assessment of its security risks from network traffic to its critical servers and identify how IDPS coverage (for both encrypted and unencrypted traffic) should be best applied to such traffic;**
- b. based on the review and assessment of security risks, implement IDPS coverage to address all network traffic flowing to its critical servers;**
- c. maintain an active license for its IDPS device and update the signatures on the device as soon as they are released by the vendor;**
- d. regularly backup the configuration files for the IDPS device and store the backup files offsite in a secure environmentally controlled location; and**
- e. limit remote administrative access to the IDPS device to authorized sources that require such access.**

**Finding 4**

**JIS had not installed malware protection software on 151 servers and also lacked assurance that malware protection software was installed on all of its workstations.**

**Analysis**

Malware protection software was not installed on most servers, and JIS also lacked assurance that malware protection software was installed on all of its workstations.

- Malware protection software was not installed on most JIS servers. JIS personnel advised us that the malware protection software was only installed on certain publicly facing servers (for example web servers). We determined that, as of November 2, 2015, 151 of 179 JIS servers which should have been protected by malware protection software did not have such software installed.
- JIS lacked assurance that malware protection software was installed and operational on all of its workstations. We identified 203 of the 5,434 total JIS workstations that either did not have malware protection software installed or the installed software was not operational.

The Administrative Office of the Courts Judicial Information Systems' *Information Security Policy* states that JIS must protect against malicious code, virus or malware, by implementing procedures and solutions that, to the extent possible, include a capability for automatic updates.

**Recommendation 4**

**We recommend that JIS ensure that all of its computers (both servers and workstations) which should be protected by malware protection software are protected by such software.**

**Finding 5**

**Numerous contractors had unnecessary network-level access to critical JIS computers, and 42 publicly accessible servers were located in the internal JIS network thereby exposing other computers in the internal network to increased risk of attack.**

**Analysis**

Numerous contractors had unnecessary network-level access to critical JIS computers, and 42 publicly accessible servers were located in the internal JIS

network thereby exposing other computers in the internal network to increased risk of attack.

- Contractors had unnecessary network-level access to the JIS mainframe computer and numerous JIS workstations. JIS was developing two significant systems with extensive use of untrusted contractors. These contractors worked on site at JIS headquarters. We determined that 30 of these on-site contractors had unnecessary network-level access to the JIS mainframe and numerous headquarters workstations.
- Forty-two publicly accessible servers were located in the JIS internal network thereby potentially exposing the other JIS computers in the internal network to increased risk of attack. These 42 servers, if compromised, could expose the internal network to attack from external sources. These 42 servers were deliberately placed in the internal network to address network response time issues between these servers and backend database servers. However, JIS did not institute compensating security controls, such as additional firewall protections, to protect these 42 servers from attack.

#### **Recommendation 5**

**We recommend that JIS**

- a. restrict each contractor's network-level access to only those servers and workstations that each contractor needs to access, and**
- b. implement compensating security controls to protect the aforementioned 42 servers from attack.**

## **Audit Scope, Objectives, and Methodology**

We have audited the Judicial Information Systems (JIS) operated by the Judiciary. Fieldwork associated with our audit of JIS was conducted during the period from September 2015 to March 2016. 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 JIS' internal control over its data center 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 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), as well as an assessment of the security controls related to JIS' use of malware protection software to protect JIS' computers. We also determined the status of the findings included in our preceding audit report on JIS.

JIS' fiscal operations are audited separately as part of our audit of the Judiciary. The latest report on the Judiciary was issued on July 16, 2013.

To accomplish our objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of JIS' 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.

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.

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 JIS' 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 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 the Judiciary 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**



August 10, 2016

MARY ELLEN BARBERA  
Chief Judge

Thomas J. Barnickel III, CPA,  
Legislative Auditor  
Office of Legislative Audits  
State Office Building, Room 1202  
301 West Preston Street  
Baltimore, MD 21201

Dear Mr. Barnickel:

We are in receipt of the Legislative Auditor's letter dated July 21, 2016, pertaining to the findings from the audit of the Judiciary's Judicial Information System. The following responds to those findings:

### **Finding 1**

**The Judicial Information Systems (JIS) maintained a circuit court database which contained 150,454 unique social security numbers with names and (in some cases) dates of birth without adequate safeguards.**

### **Recommendation 1**

**We recommend that JIS**

- 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.

### **Response:**

Concur. The Judiciary currently operates several legacy systems that may not be technically compatible with encryption or masking technology. These systems will be replaced by the Maryland Electronic Courts (MDEC) system over the next 5 years, and remediation of sensitive PII data in this system will be addressed.

- a. An inventory of systems and the identification of PII within those systems has been completed and will continue on an ongoing basis.

*Anticipated Completion: **Completed.***

- b. A review of the identified PII is being performed to determine the necessity of retaining the identified PII data in each system. All unnecessary PII data will be deleted.

*Anticipated Completion: **12/31/16***

- c. JIS has substantive security controls in place, including role based access controls, database change and system log monitoring, network security event monitoring, and real-time security alerts. The remediation of OLA findings 2, 3, and 4, will further enhance JIS' security posture.

*Anticipated Completion: **12/31/16***

Further protection of PII, by encryption or other data-centric methods, such as Data Loss Prevention (DLP), is dependent on the technical feasibility associated with some legacy systems and the Judiciary's fiscal ability to acquire the needed resources, including software, hardware and services. Estimated funding to implement additional measures will be included in the Judiciary's fiscal year 2018 budget request.

*Anticipated Completion: **6/30/18***

- d. Should, in accordance with item c., encryption be deemed an appropriate means of safeguarding information, JIS will use standards-based encryption methods to encrypt PII.

*Anticipated Completion: **6/30/18***

## **Finding 2**

**Network devices, used to help protect the JIS network, were not configured to adequately secure connections from untrusted sources and were not properly monitored, and password controls did not properly protect the perimeter firewalls.**

## **Recommendation 2**

**We recommend that JIS**

- a. configure its firewalls and routers to achieve a "least privilege" security strategy giving individuals, entities, and devices only those network access privileges needed to perform assigned tasks (repeat);
- b. configure the firewalls to send automatic email alerts to administrators concerning high severity firewall operational events;
- c. regularly review the firewalls' logs using automated tools, and investigate unusual and suspicious items, with such reviews and investigations being documented and retained for future reference; and
- d. enable the firewalls' available password control settings to meet the requirements of the State's Information Security Policy.

## **Response:**

Concur. Remediation has been in process via the implementation of upgraded firewall appliances. It should be noted that the review and reconfiguration of security rules associated with external justice partners will require close collaboration and support with the partners to meet the anticipated completion dates.



- a. JIS has procured, configured and implemented a next-generation firewall (NGFW) that is employing the “least privilege” security strategy and for adequately securing connections into the network. As part of the implementation of the NGFW, JIS has initiated a systemic review of its firewall and router rules and has removed outdated rules. In addition, JIS has reconfigured many of the firewall and router rules to adequately secure connections into the network. Eliminating and reconfiguring the remaining rules includes external justice partners, and requires close collaboration and support with the partners.  
*Anticipated Completion: December 31, 2016.*
- b. JIS has configured the network device and firewall management dashboards to generate automated email alerts for high severity firewall operational events that impact the health and security of the JIS Network. Designated JIS staff regularly review the firewall management dashboard for operational and security events.  
*Anticipated Completion: Completed.*
- c. JIS has implemented a formal process to regularly review the NGFW logs using automated tools and investigates unusual and suspicious operational and security events. A formal process for retaining all review and investigation documentation has been implemented.  
*Anticipated Completion: Completed.*
- d. JIS has refined the firewall password control settings to ensure compliance with the security policy.  
*Anticipated Completion: Completed.*

### **Finding 3**

**Intrusion detection prevention system (IDPS) coverage for the network was not effectively deployed. In addition, updates to the IDPS device and backups of the device configuration were not adequately performed or controlled, and administrative access to the device was not properly restricted.**

### **Recommendation 3**

**We recommend that JIS**

- a. perform a documented review and assessment of its security risks from network traffic to its critical servers and identify how IDPS coverage (for both encrypted and unencrypted traffic) should be best applied to such traffic;
- b. based on the review and assessment of security risks, implement IDPS coverage to address all network traffic flowing to its critical servers;
- c. maintain an active license for its IDPS device and update the signatures on the device as soon as they are released by the vendor;
- d. regularly backup the configuration files for the IDPS device and store the backup files offsite in a secure environmentally controlled location; and
- e. limit remote administrative access to the IDPS device to authorized sources that require such access.

**Response:**

Concur. Remediation has been in process via the implementation of upgraded firewall appliances.

- a. With the implementation of NGFW solution, an intrusion detection prevention system (IDPS) is in place to inspect and prevent malicious traffic from coming into the JIS network. A documented review and assessment is underway of the security risks from network traffic to critical servers and for identifying how IDPS coverage (for both encrypted and unencrypted traffic) could be further optimized and best applied.

*Anticipated Completion: **October 31, 2016***

- b. Based on the review and assessment of security risks, JIS will optimize IDPS coverage to address all network traffic flowing to its critical servers.

*Anticipated Completion: **October 31, 2016.***

- c. JIS has active licenses for its IDPS devices and has a process in place for updating signature files when the files are released by the vendor.

*Anticipated Completion: **Completed.***

- d. JIS has formalized a procedure to review and update the NGFW configuration files, and has established a process to perform nightly backups of the configuration files which are stored offsite.

*Anticipated Completion: **Completed.***

- e. JIS has limited remote administrative access to authorized personnel through secure protocols and fixed IP's of the authorized individual's workstation.

*Anticipated Completion: **Completed.***

**Finding 4**

**JIS had not installed malware protection software on 151 servers and also lacked assurance that malware protection software was installed on all of its workstations.**

**Recommendation 4**

**We recommend that JIS ensure that all of its computers (both servers and workstations) which should be protected by malware protection software are protected by such software.**

**Response:**

Concur.

Malware protection on all servers has been implemented with the NGFW solution. In addition, JIS has implemented detection software to identify workstations on the JIS Network that do not have an active threat detection/prevention agent running. A formal process for investigating, documenting and remediating all missing agents identified through this software has been developed and implemented.

*Anticipated Completion: **Completed.***

**Finding 5**

**Numerous contractors had unnecessary network-level access to critical JIS computers, and 42 publicly accessible servers were located in the internal JIS network thereby exposing other computers in the internal network to increased risk of attack.**

**Recommendation 5**

**We recommend that JIS**

- a. restrict each contractor's network-level access to only those servers and workstations that each contractor needs to access, and
- b. implement compensating security controls to protect the aforementioned 42 servers from attack.

**Response:**

Concur.

- a. Contractors employed by the Judiciary are an extension of the Judiciary personnel workforce. These individuals are subject to the same Judiciary use and non-disclosure agreements, background checks, security policies, procedures, and management supervision. Using capabilities within the NGFW solution, JIS will explore implementing additional controls on contractor access to critical computers.

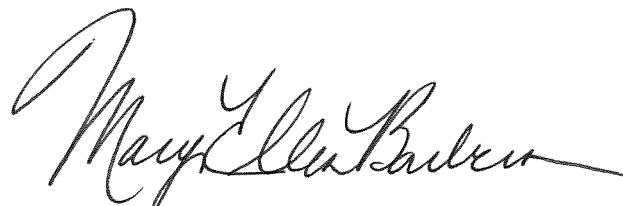
*Anticipated Completion: June 30, 2017*

- b. JIS is implementing compensating security controls to protect publicly accessible servers.

*Anticipated Completion: October 31, 2016.*

Please contact Pamela Harris, State Court Administrator, 410-260-1295, should you have further questions or concerns. Thank you for your careful consideration of the Judiciary's Judicial Information System.

Sincerely,

A handwritten signature in black ink, reading "Mary Ellen Barbera". The signature is fluid and cursive, with the first name "Mary" and last name "Barbera" being the most prominent parts.

Mary Ellen Barbera  
Chief Judge, Maryland Court of Appeals

AUDIT TEAM

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

**Michael K Bliss, CISA**  
**Edwin L. Paul, CPA, CISA**  
Information Systems Senior Auditors

**Steven D. Bryant**  
**Robert H. Dean**  
**Edward O. Kendall**  
Information Systems Staff Auditors