Washington State Judicial Branch
2023-25 Biennial Budget
Modernize Cyber Security Program

Agency: Administrative Office of the Courts

Decision Package Code/Title: R3 – Modernize Cyber Security Program

Agency Recommendation Summary Text:
The Administrative Office of the Courts (AOC) requests 3.0 FTEs and $1.7 million of General Fund-State funding per biennium to modernize AOCs cyber security efforts by implementing two programs:

- The Information Security Program will implement administrative controls by creating new processes such as Contract Security and Security Design Reviews to increase AOC's cyber threat defensive posture, threat detection, and vulnerability mitigation capabilities by implementing industry-recognized cyber security standards.
- The Risk Management Program will allow AOC to have visibility on and correlate events across multiple systems. This includes automating incident responses, which is essential to mitigating the risks of current cybersecurity threats as well as documenting risks and reducing silos.

AOC Cyber Security staff is ill-equipped to handle any intrusion or semi-sophisticated cyber-attack against the AOC or the courts of Washington, since there is limited visibility at the enterprise level due to lack of staff and tools. Cyber-attacks are becoming more pervasive and more sophisticated and the AOC must acquire and develop new capabilities to properly address cyber security attacks and issues as they develop. (General Fund-State)

Fiscal Summary:

	FY 2024	FY 2025	Biennial	FY 2026	FY 2027	Biennial
Staffing						
FTEs	3.00	3.00	**3.00**	3.00	3.00	**3.00**
Operating Expenditures						
Fund 001-1	$897,400	$810,000	**$1,707,400**	$810,000	$810,000	**$1,620,000**
Total Expenditures						
	$897,400	**$810,000**	**$1,707,400**	**$810,000**	**$810,000**	**$1,620,000**

Package Description:
As a government entity, the Administrative Office of the Courts recognizes that its information technology operations are subject to vulnerabilities and attacks and we must continue to mature our cyber security program to safeguard the judicial branch's information technology systems, as well as the data of individuals that are involved in Washington's judicial system.

The Administrative Office of the Courts must invest further to build a stronger information security program. This decision package seeks to grow capabilities and provide staff with actionable safeguards to increase the Administrative

Office of the Courts overall cybersecurity posture. This will be accomplished by implementing one of the most well-regarded industry security standards, the Center for Internet Security (CIS) Critical Security Controls (CSC)[1] framework.

The Administrative Office of the Courts must meet many regulatory requirements because of the type and sensitivity of data that is submitted and processed by the courts. As an example, because the Administrative Office of the Courts offers credit card payment portals in certain programs, the agency must comply with Payment Card Industry Data Security Standard[2] (PCI DSS). In addition, because some data processed within the agency is derived from law enforcement sources, the agency must comply with Department of Justice (DOJ) Criminal Justice Information Services (CJIS) Security Policy v. 5.9[3]. The Administrative Office of the Courts Cyber Security Staff must continue to invest in its Cyber Security program to ensure compliance with all of these regulatory requirements.

The AOC seeks funding to acquire the following products and services:

A. Security Information and Event Management (SIEM) license to allow for the correlation of technical event logs across multiple systems. Also purchase the service of a Managed Detection and Response (MDR) provider to deliver 24/7/365 outsourced monitoring of the agency's network.

B. Governance, Risk Management and Compliance (GRC) software with a license for unlimited users and unlimited risks.

C. Risk-Based Vulnerability Management (RBVM) software

The Administrative Office of the Courts would also create three (3) permanent FTEs to strengthen the Judicial Branch Cyber Security capabilities. These positions would be:

A. Cyber Security Analyst - Evaluate technical security controls against the approved standards, conduct Risk assessments on new and current applications, enhance the Security Design Review process for all Cloud or on-prem new systems/applications, and recommend changes to existing systems/applications to ensure the agency is not allowing unacceptable risk.

B. Application Security Engineer - Work closely with business and developer teams to promote secure code development by providing security requirements throughout the development process and perform Security assessments, with and without source code access, and document findings and architectural issues.

C. Cyber Defense Analyst - Configure the SIEM platform in coordination with the vendor to include the integration of event sources, monitor incoming events using security management tools. Identify, categorize, prioritize, and investigate correlated events. Perform investigation and triage of events and incidents and escalate according to established processes.

Together, these software platforms and new staff will allow the Administrative Office of the Courts to establish a more robust Risk Management Program. Individually, each of these items will provide significant enhancement from the

[1] https://www.cisecurity.org/controls
[2] Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards
[3] https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

current Administrative Office of the Courts cyber capabilities and visibility over the system comprising the Judicial Branch Enterprise. Together, they will enable Administrative Office of the Courts to move to a more proactive stance in our overall Cyber Security posture.

The Program is composed of the following endeavors:

a. Security Information and Event Management (SIEM)
There are numerous tools and event logs that record activity in our applications, within the agency's networks, and data traffic in and out of AOC. However, these logs are mostly separate, making it extremely difficult to correlate information to identify suspicious activity or patterns. A SIEM solution aggregates data from all logs and monitors, analyzes data, and provides analytics and threat assessments across all operations.

As attacks can occur at any time, this software tool will allow the continual detection and response to potential cyberattacks. The provision of a Managed Detection and Response (MDR) service provider will allow the agency to conduct 24/7/365 continuous monitoring, active hunting, and deep forensic analysis using cyber threat intelligence. An MDR solution will provide a comprehensive process for detecting cyber threats, and enhance our approach to events and incident investigation and analysis.

b. Risk-Based Vulnerability Management (RBVM)
Currently the cyber staff receives threat intelligence information from our trusted - Federal, State and industry recognized cyber security associations - partners via email. The staff evaluates the information received manually. This is time consuming and relies on staff's availability to take actions.

The RBVM software tool will allow the agency to evolve from a manual to an automated threat intelligence information gathering and quickly respond to critical vulnerabilities. It also will provide a single management system to analyze and prioritize current vulnerabilities based on severity, asset value, and threat intelligence, enabling our staff to better protect the agency and to focus on patching the most vulnerable systems.

c. Governance, Risk Management, and Compliance (GRC) platform
A GRC software platform is used to manage operations to ensure that compliance and risk standards are being met by all information technology components. The GRC platform will make it much easier to manage security policies, and conduct internal audits and risk assessments to reduce the agency's overall operational risk. The GRC platform would create a single repository for recording, analyzing, and remediating risks throughout our entire organization, providing greatly increased visibility, correlation, and remediation activities as an enterprise. This will result in a unified operational strategy and consistent operations across the agency, and will give the management team a view of the organization as a whole, and therefore, be better positioned to make more informed business decisions.

Implementing a GRC framework will allow the agency to have a centralized approach to governance, risk management, and compliance that will speed up information gathering processes and improve the quality of the data collected.

Fully describe and quantify expected impacts on state residents and specific populations served:
As the cyber threat landscape is constantly changing and evolving, implementation of these programs and tools will allow the Administrative Office of the Courts and the Cyber Security Unit to stay a step ahead by continuing to improve the ways in which it secures the Courts' data, therefore benefiting everyone as a whole.

Explain what alternatives were explored by the agency and why they were rejected as solutions:
This request is to establish three new software-based capabilities in the Administrative Office of the Courts' Cyber Security Program through a market analysis and procurement process. The complexity of the cyber security capabilities does not allow manual processes or other substitutes to accomplish the necessary work in an efficient or effective manner.

What are the consequences of not funding this request?
If this request is not funded, the Administrative Office of the Courts will continue to perform these critical cyber security processes manually. This means that investigations of cyber security incidents will produce actionable results only after too much time has passed to rapidly correct issues. It would also prevent the agency from establishing proactive processes to identify issues or attacks right as they are beginning. Instead, the agency's Cyber Security program will continue in a reactive mode for many incidents.

Is this an expansion or alteration of a current program or service?
This is an expansion of the Administrative Office of the Courts' Cyber Security program. Over the last five years, the agency has established its Cyber Security program and integrated it into many function in the agency. This request will establish three new capabilities that will help transition the agency's cyber security stance from reactive to proactive.

Decision Package expenditure, FTE and revenue assumptions:

Staffing Assumptions

Senior IT Security Analysts. Beginning July 1, 2023 and ongoing, AOC requires salary, benefits, and associated standard costs for 3.0 FTE to fulfill the roles of Cyber Security Analyst, Application Security Engineer, and Cyber Defense Analyst.

Other Non-Standard Costs
Purchased Services, Software and Licensing (Object E)
One-time and ongoing funding will also be needed for software products and licenses and professional services.

SEIM and MDR. FY 2024 One-Time: $60,000 training and onboarding. Ongoing beginning FY 2024: $172,000 software and licensing per fiscal year

RBVM. FY 2024 One-Time: $8,000 training and onboarding. Ongoing beginning FY 2024: $31,000 software and licensing per fiscal year

GRC. Ongoing beginning FY 2024: $16,000 software and licensing per fiscal year

Expenditures by Object		FY 2024	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029
A	Salaries and Wages	334,500	334,500	334,500	334,500	334,500	334,500
B	Employee Benefits	106,700	106,700	106,700	106,700	106,700	106,700
E	Goods and Services	320,400	247,400	247,400	247,400	247,400	247,400
G	Travel	7,500	7,500	7,500	7,500	7,500	7,500
J	Capital Outlays	19,200	4,800	4,800	4,800	4,800	4,800
T	Intra-Agency Reimbursements	109,100	109,100	109,100	109,100	109,100	109,100
	Total Objects	**897,400**	**810,000**	**810,000**	**810,000**	**810,000**	**810,000**

Staffing

Job Class	Salary	FY 2024	FY 2025	FY 2026	FY 2027	FY 2028	FY 2029
SENIOR IT SECURITY ANALYST	111,500	3.00	3.00	3.00	3.00	3.00	3.00
Total FTEs		**3.00**	**3.00**	**3.00**	**3.00**	**3.00**	**3.00**

Explanation of standard costs by object:
Salary estimates are current biennium actual rates at Step L.
Benefits are the agency average of 31.89% of salaries.
Goods and Services are the agency average of $3,800 per direct program FTE.
Travel is the agency average of $2,500 per direct program FTE.
One-time IT Equipment is $4,800 for the first fiscal year per direct program FTE. Ongoing Equipment is the agency average of $1,600 per direct program FTE.
Agency Indirect is calculated at a rate of 24.73% of direct program salaries and benefits.

How does the package relate to the Judicial Branch principal policy objectives?
This package directly advances the Judicial Branch policy objective of Sufficient Staffing and Support. Cyber Security is a critical program in the provision of any information technology services. An efficient and effective program is absolutely vital to support the operation of all of the Administrative Office of the Courts' information technology systems and to support the smooth operation of the courts of the state, as well as ensuring court data is available to other state agencies.

Are there impacts to other governmental entities?
This request will benefit trial courts, appellate courts, and state agencies such as Washington State Patrol and the Department of Licensing. Increasing the capabilities of the Administrative Office of the Courts' Cyber Security program benefits all stakeholders by enhancing the agency's ability to prevent, detect, and respond to cyber security incidents like hacks, leaks, and vulnerabilities. The Administrative office of the Courts expects support of this request from other government entities.

Stakeholder response:
No non-governmental stakeholders will be impacted by this proposal.

Are there legal or administrative mandates that require this package to be funded?
There are no legal or administrative mandates that require that this package be funded.

Does current law need to be changed to successfully implement this package?
No changes to current law are required to successfully implement this package.

Are there impacts to state facilities?
This request does not impact any state facilities.

Are there other supporting materials that strengthen the case for this request?
There are no other supporting materials included in this package.

Are there information technology impacts?
Approval of this request would result in the Administrative Office of the Courts procuring new commercial software packages or additional modules for software products already in use at the agency to establish new Cyber Security capabilities. The IT-related costs would include contract with service providers, software licensing, and hardware costs.

Agency Contacts:
Christopher Stanley, 360-357-2406, christopher.stanley@courts.wa.gov
Angie Wirkkala, 360-704-5528, angie.wirkkala@courts.wa.gov