WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

State Office of Cybersecurity Catalog of Services Report

July 2022

Table of contents

Introduction

Senate Bill 5432 (2021), established WaTech's Office of Cybersecurity (OCS) as the state's lead organization to develop centralized state government security services.

OCS, in collaboration with state agencies, is required to develop a catalog of cybersecurity services for OCS to perform. The information is required to be submitted in a report to the Legislature and governor by July 1, 2022.

As required under RCW 43.105.460, this report must include, but not be limited to:

a) Cybersecurity services and functions to include in the Office of Cybersecurity's catalog of services that should be performed by the Office of Cybersecurity;

b) Core capabilities and competencies of the Office of Cybersecurity;

c) Security functions which should remain within agency information technology security programs;

d) A recommended model for accountability of agency security programs to the Office of Cybersecurity; and

e) The cybersecurity services and functions required to protect confidential information transacted, stored, or processed in the state's information technology systems and infrastructure that is specifically protected from disclosure by state or federal law and for which strict handling requirements are required.

This report is divided into four sections:

Section One – Executive Summary: Provides a high-level overview of the report, with summary of current capabilities and recommendations.

Section Two – OCS Enterprise Services: This section describes current OCS enterprise capabilities, discusses future security needs, and provides recommendations for services to be shared by OCS and agencies or remain at the state agency level.

Section Three – Foundational Cybersecurity Support Services: A brief overview of services WaTech offers in other areas of its operations that contribute to the state's security posture, such as the state's virtual private network (VPN). While these services are not a primary support responsibility for OCS, the office guides requirements and ensures that policies, configurations, and metrics are tracked and evaluated.

Section Four – Accountability model for agency security programs: The state of Washington has historically had a federated IT environment with each agency largely responsible for its own systems. This section outlines the importance of strong governance and collaboration between agency cybersecurity programs and OCS and provides an overview of the governance model deployed to ensure effective cybersecurity in the state now and into the future.

Section One: Executive Summary

With more than 100 state agencies serving a population of nearly eight million people, the state of Washington has one of the largest and fastest growing service delivery systems in the nation. State agencies utilize a vast number of information technology systems to provide services to Washingtonians and protect their data.

The state has evolved from systems predominantly residing in the state data center and utilizing the State Government Network (SGN) to a more distributed system environment that uses the public cloud and vendor data center environments.

Accelerated by work-from-home initiatives during the COVID-19 pandemic, the state workforce has modernized toward accessing the SGN and cloud services from the office and home using the internet. Agencies have also adopted technology allowing for higher risk transactions – that used to require an in-person visit – to be done remotely.

This change in how the state does business requires a more mature approach and increase in the use of enterprise security services. This will improve protection of state technology systems and the large amount of data residing there throughout its lifecycle.

As a result of these changes and the passage of Senate Bill 5432 (RCW 43.105.460), OCS implemented enterprise security services in 10 focus areas for state agencies such as endpoint security and risk and compliance management. (WaTech for many years also has provided other services in other areas of its operations that contribute to the state's security posture, such as the state's virtual private network (VPN), but they are not administered by OCS. These services are described in more detail in Section Three.)

Section Two of this report provides an overview of the 10 new enterprise security platforms provided by OCS as well as recommendations for future enterprise capabilities. The section also discusses the security responsibilities and needs for OCS and state agencies.

State agencies were actively engaged in the creation of this report. They provided feedback to WaTech on the current enterprise platforms as well as advice on services that could be offered in the future.

All the enterprise services described in this report need to be matured and improved. WaTech will evaluate the need for additional funds and put forward decision packages as required. An overarching theme is the need to increase the automation in the current tools to speed up reaction times. The platforms and tools summarized below represent best practices and are fundamental to any enterprise cybersecurity program:

1. Endpoint Security: OCS uses Microsoft's Endpoint Detection and Response (EDR) system to monitor and mitigate security issues and threats on a variety of device types – servers, laptops, tablets, mobile phones, etc. The system is used to identify threat patterns, automatically remove or contain threats and notify security personnel. Use of the EDR is currently a largely manual process. Given the growing speed and sophistication of cyberattacks, EDR environment automation would significantly enhance the state's security posture. This would require staff training, reorganizing and assigning responsibilities for the enhancements.

2. **Security Information and Events Management:** The state's cloud-based Security Information and Event Management (SIEM) platform collects logs (such as unauthorized attempts to log into state systems) that provide critical information about what's happening in the state's IT systems. A SIEM analyzes and correlates log data, allowing the state to identify the source of an attack and its effects on IT systems. As with Endpoint Security, the state can significantly improve its security posture by automating the detection, response, and remediation of security incidents.
3. **Vulnerability Management:** The vulnerability management program (VMP) scans for weaknesses in state systems that bad actors target and helps agencies prioritize and remedy those weaknesses. Bad actors can exploit vulnerabilities to upload malicious software – including ransomware – to conduct attacks. The VMP provides an enterprise view of vulnerabilities, the potential risks associated with them and a path to prioritize remediation activity across hundreds of thousands of devices. The VMP needs to be integrated into the SIEM to reduce potential risk and consolidate vulnerability information reporting via dashboards to enhance visibility. This would require staff training, reorganization and assigning responsibilities for the enhancements.
4. **Security Incident Management:** Incident management consists of detecting security incidents and assisting with remediation and recovery. The OCS Security Operations Center (SOC), using the enterprise security platforms described in this report, works to proactively identify threats and alert agencies. The OCS Computer Incident Response Team (CIRT) helps determine the severity of incidents and assists agencies with remediation and restoration of services. OCS needs to implement runbooks, playbooks, and training exercises to mature its incident management program.
5. **Threat Detection & Intelligence:** OCS receives intelligence from its security vendors and federal partners about security threats. That information is manually fed by security staff into enterprise security platforms and shared with agencies for awareness and for integration into their security tools. Threat intelligence is key to proactively preventing malicious activity and identifying potential threats in our IT systems. OCS will mature its capabilities by acquiring an enterprise-wide threat intelligence platform that can automatically integrate threat intelligence feeds into security tools, which would reduce the time it takes to identify and mitigate threats. OCS also needs additional tools to create traps that lure attackers into isolated networks so security staff can safely observe their actions and attempt to reverse engineer attacks.
6. **Threat Hunting:** OCS security analysts currently use a SIEM (see #2 above) capability to aggregate log information to hunt for suspicious activity. The tool alerts staff when it finds potentially malicious activity. Much of the threat hunting is a manual process. OCS needs to automate the process of hunting for common attack methods and alerting staff. This would speed up detection and response times and free up staff to look for more sophisticated threats.
7. **Risk & Compliance Management:** While OCS has a VMP (see #3 above) and provides a security assessment service to validate the controls deployed on agency systems, the office does not have the ability to analyze existing cybersecurity risk and compliance with controls at an enterprise level. Agencies follow their own risk analysis and oversight process related to special

data handling requirements, such as the federal Health Insurance Portability and Accountability Act (HIPAA). This creates inconsistencies that limit the analysis of how agency-level risk impacts the state overall. OCS needs a Governance Risk and Compliance (GRC) solution for the assessment, reporting and management of cybersecurity risks that augments the existing security design review process. This GRC solution will enable agencies to perform risk and compliance management consistently .

8. **Application Security:** Agencies that develop or deploy applications must address security as part of their IT operations and software development lifecycle. Online applications, where users interact with state systems, create elevated risk because internet access provides a path for attacks. In response, OCS has put in place an enterprise web application firewall (WAF) service which is focused on the highest-risk applications. This leaves other high-risk and medium risk applications without the needed protection. Three services are needed to address this gap: 1) A cost-effective enterprise WAF solution for mid-range applications hosted on-premises or in cloud environments; 2) an application code scanning service to mitigate weaknesses introduced during the development phase; and 3) an application vulnerability scanning solution that scans for and identifies security issues in running applications. These three services will provide a layered approach to mitigating application security issues and are key to addressing cyber risk for the state.
9. **Data Security:** Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. OCS partners with the Office of Privacy and Data Protection (OPDP) to provide statewide direction to agencies in terms of best practices in data encryption methods, state privacy laws, best practices in managing confidential information and other tools and resources. WaTech also provides an enterprise backup service for agencies which can be used. Agencies must ensure backups are secure for data they own and manage.
10. **Network Perimeter:** A key aspect of maintaining the security of the state network is monitoring for and mitigating malicious internet traffic. The OCS security operations center (SOC) has deployed security solutions at the network perimeter that provide intrusion detection and prevention, denial of service mitigation and zero-day malware protection. These solutions work in concert with WaTech enterprise firewalls and form the foundation of the layered network security model used to protect the state network.

It is critical that the state establishes centralized governance and controls to ensure that enterprise services and infrastructure remain secure. The state historically has had a federated IT environment with each agency largely responsible for its own systems. As technology has evolved and increased in complexity, so has the need to move to a different type of IT operating model.

To ensure accountability of agency cybersecurity programs (RCW 43.105.460(1)(d)) to the Office of Cybersecurity, WaTech has created an Enterprise Security Governance (ESG) Council, chaired by the state Chief Information Security Officer (CISO). This council will focus on the development, deployment, and refinement of enterprise security services. OCS, in coordination with the council, will implement an operations plan to mature the state's IT security efforts and steadily improve the state's security posture.

Section Two: OCS Enterprise Services

The state is moving away from a federated approach to cybersecurity – where each state agency is largely responsible for its own IT security – to an enterprise approach, as appropriate, to manage risk. This section describes current OCS capabilities, what is needed to continue improving the state's enterprise security posture, capabilities required at the state agency level, and future steps. WaTech will evaluate the need for additional funds and put forward decision packages as required.

Current OCS enterprise capabilities:

1. Endpoint Security
2. Security Information and Events Management
3. Vulnerability Management
4. Security Incident Management
5. Threat Detection & Intelligence
6. Threat Hunting
7. Risk & Compliance Management
8. Application Security
9. Data Security
10. Network Perimeter

Endpoint security

Current capabilities: WaTech's Office of Cybersecurity (OCS), in coordination with state agencies, deployed an enterprise-level Endpoint Detection and Response (EDR) system in response to security incidents during 2020. The software, for the first time, provided the state with enterprise-wide visibility and security capability. Most state agencies are using the enterprise solution. The EDR combines continuous monitoring and collection of data with automated response and analysis capabilities for system endpoints – servers, laptops, tablets, mobile phones and other wireless devices. The types of threats blocked include malicious applications and scans by bad actors searching for vulnerabilities. The main purpose of the system is to monitor and collect information that could indicate a threat, analyze the information and inform security personnel.

Future capability: Use of the EDR is currently a largely manual process executed by security staff. Given the growing speed and sophistication of cyberattacks, the use of more advanced technology to automate the EDR environment would significantly enhance the state's security posture. Emerging technology will enhance the EDR system, allowing security analysts to automate processes.

Responsibilities & needs:

	Responsibilities	Needs
OCS	• Monitor hardware and software to ensure it is reporting alerts to the SIEM. • Follow up on alert status and remediation efforts at state agencies. • Coordinate response efforts and communicate findings.	• This would require staff training, reorganizing, and assigning responsibilities for the enhancements.
Agencies		• Agencies need to be integrated into the WaTech enterprise IT Service Management system (ITSM) to improve their ability to generate and track tickets.
OCS & Agencies	• Deploy EDR software on agency devices. • Validate EDR interoperability. • Triage alerts and events for routing to agency security analysts.	• Security analysts need training on configuration, operation and development of features licensed for the EDR system. • Playbooks and runbooks for common events, such as how to manage incidents. • A community repository for playbooks and runbooks. • Recurring maintenance of all documentation.

Next steps to mature capabilities:

- OCS will create a funding plan for the Endpoint system to meet enterprise needs and automate detection and response.
- Create runbooks and playbooks.

Security Information and Events Management

Current capabilities: In 2021, the state deployed a new cloud-based Security Information and Event Management (SIEM) platform that improved the ability of security staff to detect and respond to signs of attacks on state assets. The SIEM provides the state with an enterprise view of all executive branch agencies and can detect threats across the state's nearly 10,000 infrastructure assets (servers, network devices, etc.), providing detailed intelligence needed to detect and mitigate threats. The new platform, which replaced an on-premises implementation with a cloud-based system, expanded the state's ability to collect log data, including from sources not previously available. Logs provide critical information about what's happening in the state's IT system. Most agencies have committed to this service, with onboarding efforts continuing through 2023.

Future capability: As with Endpoint Security, the state can significantly improve its security posture by automating the detection, response, and remediation of security incidents. The state also needs to improve its ability to conduct continuous threat hunting across the enterprise using threat intelligence information from federal partners (including the FBI and the Cybersecurity & Infrastructure Security Agency) that's integrated into the SIEM platform. In addition, a statewide repository of playbooks and runbooks is needed that define precise actions and steps that agencies can carry out during security incidents.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Maintain a state of vigilance that protects state resources and citizens. • Improve security awareness across the enterprise. • Use the SIEM to aggregate logs and security information from the infrastructure deployed across all agencies. • Perform post incident lessons learned. • Perform post incident assessments to ensure completeness of remediation activity.	• Visibility into agency network traffic and packet payload on an as needed basis, along with packet capture tools. • Threat Intelligence platform feeds from vendor and federal and multi-state information sources.
OCS & Agencies	• Correlate information and event data into actionable tasks that are performed by security analysts at OCS and state agencies. • Provide data to the OCS Computer Incident Response Team (CIRT) for containment, removal and remediation of malicious activity and malware.	

Next steps to mature capabilities:

- OCS will create a funding plan for the system to meet enterprise needs.
- OCS and agencies work on improvement plan via the enterprise security governance council.

Vulnerability Management

Current capabilities: The vulnerability management program (VMP) scans for the same weaknesses in state systems that bad actors look for and helps agencies to prioritize and remedy those weaknesses before they can be exploited. Threat actors can exploit vulnerabilities to upload malicious software – including ransomware – to conduct attacks. The VMP provides the state with an enterprise view of vulnerabilities, the potential risks associated with them and a path to prioritize remediation activity across hundreds of thousands of devices. The VMP was implemented in response to security incidents during the COVID-19 pandemic which identified the need for an enterprise-wide tool and visibility. This solution avoids a patchwork approach where agencies are using different solutions that impede visibility. When agencies operate in silos, it increases the risk of missed intelligence that could expose system vulnerabilities. For example, patching and ensuring systems are properly configured are two primary factors that help us keep our systems safe. The VMP excels in this arena.

Future capability: The VMP needs to be integrated into the Security Information and Event Management (SIEM) system. This would allow for consolidated reporting dashboards and automated response to critical alerts. Automate the actions that staff execute for repeatable processes to help ensure smooth operations.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Management and maintenance for software platforms. • Scan agency environments scheduled and as needed. • Generate and disseminate incident reports.	• Dashboard development and training to generate and display metrics. • VMP integration with threat hunting tools. • VMP integration with incident response tools. • System management and maintenance. • Development of playbook and runbook for managing incidents and creating a repository for documentation. • Document management and development.
Agencies	Generate and disseminate incident reports.	
OCS & Agencies	Track remediation of incidents for completeness and improvements.	

Next steps to mature capabilities:

- OCS will create a funding plan for the system to meet enterprise needs.
- OCS will develop a process improvement document for use by the enterprise.
- OCS and agencies will work on an improvement plan via the enterprise security governance council.

Security Incident Management

Current capabilities: Incident management consists of detecting security incidents and assisting with remediation and recovery. The OCS Security Operations Center, using a suite of enterprise platforms works to proactively identify threats and alert agencies. In addition, state law requires agencies to report incidents to OCS within 24 hours of detecting an incident independently. The OCS Computer Incident Response Team (CIRT) works with the impacted agency to determine the severity of the incident and assist with remediation and restoration of services.

Future capability: The OCS incident management process needs to be matured, including the creation of run books, play books and policies, as well as holding training exercises to improve readiness for both OCS and state agencies. In addition, many of the security platforms currently in use have features that can be automated, but training is needed to take advantage of those features. The CIRT team needs improved capabilities, such as forensic investigations. This would require staff training and reorganizing and assigning responsibilities for the enhancements. OCS needs to create a model statewide incident management program and policy, with standardized reporting across all state agencies and performance metrics to evaluate and improve incident response effectiveness.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Detection, remediation and recovery during security incidents, along with all post incident activity such as lessons learned. • Coordinate and manage third party incident response partners. • Update the enterprise-wide policy, with input from agencies. • Mission statement, strategies and goals. • Create a standard taxonomy for defining an incident.	• This would require staff training, reorganization and assigning. responsibilities for the enhancements. • Create a dashboard with standardized metrics for reporting across agencies. • Ongoing training in the latest incident response techniques.
OCS &	• Move from a federated environment	Tools and methods to communicate during

Agencies	where individual agencies independently respond to security incidents, to more of an enterprise model where OCS plays a larger role in assisting agencies with their needs. • Internal and external communication methods. • Scheduled enterprise-wide exercises to determine gaps and needs.	security incidents outside the work email system, with the assumption that threat actors may be able to monitor email if the system is compromised.

Next steps to mature capabilities:

- OCS will create a funding plan for the system to meet enterprise needs.
- OCS will identify emerging technology that keeps pace with attack techniques.
- OCS will enhance CIRT team training related to best practices recommended by our partners.
- OCS and agencies will conduct exercises to test our ability to respond efficiently to attacks.

Threat Detection & Intelligence

Current capabilities: OCS, through its security vendors and federal partners (including CISA, FBI, MS-ISAC) receives timely intelligence about security threats on a local, regional, national, and global basis. The threat intelligence feeds into enterprise security platforms and is coordinated by OCS with agencies for awareness and for integration into their security tools. Threat intelligence is key to enhanced threat protection, including proactively preventing malicious activity and identifying potential threats in our IT ecosystem.

Future capability: OCS needs additional tools and capacity to create traps that lure attackers into isolated networks so that security staff can safely observe their actions and attempt to reverse engineer an attack. OCS also needs to mature its capabilities by acquiring an enterprise-wide threat intelligence platform that can automatically integrate threat intelligence feeds onto OCS security tools, which would reduce the time it takes to identify and mitigate threats.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Operate and maintain all the threat feeds and integrate into the SIEM. • Educate agencies on latest intelligence. • Improve efficiency in terms of threat detection.	• Create traps that lure attackers into isolated networks so that security staff can safely observe their actions and attempt to reverse engineer an attack. • Acquire an enterprise-wide threat intelligence platform that can automatically integrate threat intelligence feeds onto OCS security tools. • Infrastructure to build honeynets and honeypots.
OCS & Agencies	• Proactively prevent malicious activity. • Identify threats in IT ecosystem.	

Next steps to mature capabilities:

- OCS will create a funding plan for a Threat Intelligence platform.
- OCS will develop a process improvement document for use by the enterprise.
- OCS and agencies will conduct exercises to test our team's ability to detect threats within the enterprise.

Threat Hunting

Current Capabilities: OCS security analysts currently use an enterprise security tool to aggregate log information collected by the SIEM (see above) to hunt for suspicious activity. The tool alerts staff when it finds potentially malicious activity. While there is some automation, much of the threat hunting is a manual process.

Future capability: Automation of the security platform is needed to hunt for common attack methods and alert staff. This would speed up detection and response times and free up staff to look for more sophisticated threats.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Create playbooks and runbooks to automate common techniques of threat detection. • Assist agencies with conducting threat hunting. • Management and maintenance of tools.	• This would require staff training, reorganization and assigning responsibilities for the enhancements. • Enterprise document repository license to allow for increased use of threat hunting tools. • Repository for documentation for runbook and playbook.
OCS & Agencies	Shared responsibility for finding indicators of compromise and alerting each other and partners.	

Next steps to mature capabilities:

- OCS will create a funding plan for the system to meet enterprise needs.
- OCS will automate threat hunting processes that eradicate malware in the environment.
- OCS will develop a process improvement document for use by the enterprise.
- OCS and agencies will conduct training exercises to test our defenses.

Risk & Compliance Management

Current Capabilities: While OCS has a VMP (see above) and provides a security assessment service to validate the controls deployed on agency systems (through its Computer Incident Readiness Team). The office does not have the ability to analyze the potential impact of existing vulnerabilities at an enterprise level. Each agency individually analyzes its own level of risk and compliance with state and federal security standards. Oversight related to special data handling requirements, such as the federal Health Insurance Portability and Accountability Act (HIPAA) drive these programs. Consequently, these agencies developed custom risk management programs in response to that scrutiny. This lack of consistency hampers the analysis of how agency-level risk impacts the state overall.

Future capability: OCS plans to implement a risk assessment and risk management program for deployment in each agency that augments the existing security design review process. The program will contribute to the centralized management and analysis of agency cyber risks. OCS needs a governance, risk, and compliance (GRC) tool to consolidate information from risk assessments, control architecture, and Security Design Reviews that will enable analysis of statewide risk. This solution will enable all agencies to perform risk and compliance management in a consistent fashion. It will also enable the reporting and management of enterprise cybersecurity risks.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	Responsible for establishing and promoting a uniform risk and compliance management program for all agencies. It is also responsible for training agencies on the associated procedures.	A governance, risk and compliance (GRC) product to consolidate information from agency risk assessment, compliance requirements, and control environment.
Agencies	Responsible for applying the uniform risk and compliance program within their environments.	

Next steps to mature capabilities:

- OCS will create a funding plan for the system to meet enterprise needs.
- OCS will establish a uniform IT risk and compliance management program.

Application Security

Current capabilities: Online applications, where users interact with state systems, create risk because internet access provides a path for attacks. The state has put in place limited deployment of a vendor-managed enterprise web application firewall service which is effective at mitigating malicious activity. However, it is focused on a small number of high-risk applications due to the high cost of the solution. This leaves other high-risk applications as well as mid-level risk applications without the needed protection. In addition, there is no enterprise service for scanning applications for security weaknesses, or for source code security scanning during development. Agencies currently must identify the need, allocate funding and select an appropriate vendor. This has resulted in limited use of source code scanning and application security scanning tools increasing the risk of vulnerabilities in code or applications not being identified on an on-going basis.

Future capability: A layered mitigation approach is needed to address application security risks at different stages – from development when code is written to when applications are made available to the public. The code must be tested and fortified against known and emerging threats. OCS will pursue mature cloud-based enterprise solutions that are flexible and multi-tenant ready to support various agency needs and requirements. These would allow for scalable services that can be sized to the need and provide for consistent mitigation across the enterprise. Enterprise services needed to address risks include:

- ✓ Static application security testing (SAST) – Used during the development process by scanning application code to identify vulnerabilities and errors that are then mitigated before the code is put into production.
- ✓ Dynamic application security testing (DAST) – Scanning of running applications to identify

vulnerabilities in a system (that were not identified through code scanning alone). This simulates malicious activity and techniques used by attackers to identify security weaknesses.

- ✓ Web application firewalls (WAF) – A security mitigation tool that is positioned in front of applications and monitors communications to identify and block malicious activity.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Work with agencies to identify requirements and then select vendors that meet agency as well as OCS specifications. • Work with the vendors and agencies to define integrations and designs for using the enterprise services. • Staff and maintain or utilize a vendor provided service (managed or hybrid) based on solution type selected.	
Agencies	• Assist OCS in the requirements gathering and selection process. • Provide staff resources to utilize the services and identify and mitigate security issues using the tools to address cybersecurity risk.	
OCS & Agencies		Funding to build out and maintain the SAST, DAST and WAF. All three would be vendor-provided cloud solutions that provides enterprise visibility with administration delegated by OCS.

Next steps to mature capabilities:

- Establish enterprise service design based on agency and OCS requirements.
- OCS will create a funding plan to meet enterprise needs.

Data Security

Current Capabilities: Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. Three WaTech offices provide these services at the enterprise level – WaTech's Office of Privacy and Data Protection (OPDP), the Office of the Chief Information Officer (OCIO) and OCS. WaTech's OPDP provides statewide resources relating to reducing risk using data classifications, data breach law awareness, data sharing agreements templates and other resources. The OCIO and OCS provide statewide standards and best practices in the areas of data encryption, data recovery and breach investigations.

Future capability: Threats targeting our data continue to grow and the value of our data increases every day. We need to increase our ability to evaluate the security behaviors of our staff. We also need to place more emphasis on validating those critical data assets are being backed up and can be recovered in the event of a security breach or other service disruption, and we need to work to ensure that data breach investigations are performed consistently to ensure all state parties remain aware. The establishment of an Enterprise Data Governance program would also increase our state's maturity in the management and security of the data assets that are entrusted to us.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Provide assistance to agencies supporting data theft, breach and unauthorized access investigations.	• This would require staff training, reorganization and assigning responsibilities to establish an Enterprise Data Governance program. • Create a funding plan to support an Enterprise Security Awareness program for evaluating the security behaviors of our state employees.
Agencies	• Implement adequate backup routines/schedules to protect agency information assets based on its criticality to their mission and to our state. • Responsible for ensuring their data management procedures and policies are compliant with state and agency unique regulatory bodies.	• Data backup exercises need to be incorporated into recurring audits.
OCS & Agencies		Establish a consistent process for conducting data breach investigations.

Next steps to mature capabilities:

- OCS will work with our security community to develop a data breach investigation template.
- OCS will create a funding plan to operationalize an enterprise security awareness platform.
- OCS will partner with OPDP to establish an Enterprise Data Governance program.
- OCS will influence development of enterprise standards for conducting data recovery exercises.

Network Perimeter

Current Capabilities: A key aspect of maintaining the security of the state network is monitoring for and mitigating malicious internet traffic. The OCS security operations center (SOC) has deployed security solutions at the network perimeter that provide intrusion detection and prevention, denial of service mitigation and zero-day malware protection. These solutions work in concert with WaTech enterprise firewalls and form the foundation of the layered network security model used to protect the state network.

Future capability: OCS and other WaTech programs are deploying an enhanced denial of service capability that will both modernize protections in the state government network and include upstream mitigations supplied by our internet service provider to address large-scale attacks. An effort to evaluate the current intrusion detection and prevention technology will also occur to determine if security features can be combined and enhanced in an updated firewall platform.

OCS or agency responsibilities & needs:

	Responsibilities	Needs
OCS	• Monitors internet traffic and mitigates attacks using tools deployed by the security operations center and WaTech. • Alerts agencies of suspicious activity to ensure security events are researched and remediated.	• Enhanced intrusion detection and prevention tools that increase efficiency and effectiveness of mitigations.
Agencies	• Take action to resolve security alerts identified by the agency and the OCS security operations center. • Contact the OCS security operations center to research and respond to suspicious activity and incidents.	

Next steps to mature capabilities:

- OCS will take the outcome of the intrusion detection and prevention evaluation and create a funding plan to meet enterprise needs.

Section three: Foundational Cybersecurity Support Services

WaTech for many years has provided services in other areas of its operations that contribute to the state's security posture, but they are not directly administered by OCS at this time.

Foundational services include:

- SecureAccess Washington (SAW): SAW provides self-administered single sign-on access to multiple agency applications, shields online services from harmful activity, and allows access only to known users.
- Secure File Transfer: Secure File Transfer allows entities operating within the State Government Network (SGN) to securely transfer files without leaving the SGN.
- Virtual Private Network (VPN): The state VPN provides state workers and contractors with secure internet access to agency networks from any location.
- M365 Defender Functions: M365 Defender is an enterprise defense suite that provides detection, prevention, investigation, and response across identities, email and applications.
- Enterprise Active Directory: Active Directory is the shared centralized authentication and authorization service. It is a platform that provides authorization, roles and group services and enforces security policies, installs and updates software, and assists with identity management.
- Internal Certificate Authority: The Internal Certificate Authority (ICA) provides digital certificates for use inside the State Government Network to address the need to protect data in transit. Certificates issued to state agencies are used for encryption, authentication and identification of servers and/or client. Some agencies use the ICA to provide protection of sensitive data and high-value resources.

While these services are not a primary support responsibility for OCS, the office guides requirements and ensures that policies, configurations, and metrics are tracked and evaluated.

Because of their visibility and importance to the state's enterprise security posture, close collaboration across WaTech and the state's technology enterprise will be important to managing the state's security posture on an ongoing basis.

Section Four: Accountability Model for Security Programs

The state of Washington has historically had a federated IT environment with each agency largely responsible for its own systems. This approach dates to the pre-internet age – when mainframe computers were the norm – and is codified in law (see RCW 43.105.385). While WaTech is responsible for managing enterprise technology capabilities as well as utility-based infrastructure services, agencies are responsible for managing their own agency-specific application services.

This type of operating model is not unique to our state. But as technology has evolved and increased in complexity – the advent of personal computers, the internet, smartphones, and the cloud – so has the need to move to a different type of IT operating model. A federated environment, with each agency largely responsible for maintaining its systems and security, creates growing risks in an increasingly interconnected world. When agencies operate in silos, it increases the risk of missed signals that could expose system vulnerabilities. It is critical that WaTech and agencies establish centralized governance and controls to ensure that enterprise services and infrastructure remain secure.

Equally important is the use of agency cybersecurity programs embedded within individual agencies that provide awareness and insight into their needs. Cybersecurity needs will vary from agency to agency based on the type of business that an agency conducts, the type of data they store, and other unique business practices.

Managing cybersecurity effectively in this type of operating model requires strong governance structures to be established that ensure security services and capabilities are deployed thoughtfully and managed effectively.

As part of a collaborative effort to move in this direction, WaTech has established an Enterprise Security Governance (ESG) Council, chaired by the state CISO. This workgroup, which includes all executive branch agencies, has been chartered and meets monthly.

The ESG council was actively engaged in the creation of the Catalog of Services Report with representatives from agencies providing feedback to WaTech on the current enterprise platforms as well as advice on future services that could potentially be offered.

One pattern that emerged from the agency comments is the need to mature the state's existing set of services before adding new capabilities.

The council's charter will be reviewed annually, with a mechanism in place to modify the charter based on the state's needs. These timelines align with the responsibilities of agency cybersecurity programs to provide agency security business needs and program metrics on an annual basis. This rhythm of business will create an effective model for reviewing and acting on information provided to OCS by agency cybersecurity programs. With the formation of the ESG, OCS will be able to effectively partner with agency cybersecurity programs to improve security services in state government.

The council's responsibilities include:

- Focusing on the development, deployment, and refinement of enterprise security services.

- Defining roles, responsibilities, and integrations for all defined security services.
- Providing guidance, review, and subject matter expertise to OCS as it fulfills its statutory obligation to develop cybersecurity policies.
- Serving as the primary governance vehicle for security service and operations in the state and providing a structure for ongoing decision making on cybersecurity best practices, policies, and services to be deployed in the state.

Due to the variety of business needs and cybersecurity challenges across the state, membership on the ESG is comprised of agency CISOs or the other highest ranking security contact at each state agency. This composition will ensure that cybersecurity functions, services, and policies developed and approved by the ESG consider security business cases and needs that are required to protect confidential information specifically protected from disclosure by state or federal law, as well as those for which strict handling requirements exist.

The ESG will also contribute to OCS's ongoing needs related to performance management and will serve as a crucial forum to collect performance metrics to inform OCS's management of enterprise security services. The ESG will provide a forum to develop relevant, timely performance metrics for both OCS and agency security programs which will be used to inform updates to enterprise security services for the state of Washington.

Contact

For questions about this report, please contact:

Bill Kehoe
State CIO
bill.kehoe@watech.wa.gov