WaTech
Washington Technology Solutions

Catalog Of Services

State Office of Cybersecurity

Date: December 2024

Author: Ralph Johnson,
State Chief Information Security Officer

This Page Intentionally Left Blank

Table of Contents

Introduction

WaTech's state Office of Cybersecurity (OCS), established under RCW 43.105.450, oversees and enhances cybersecurity across Washington state government. As mandated by RCW 43.105.460, OCS is tasked with developing, maintaining, and regularly updating a comprehensive catalog of cybersecurity services. The 2024 catalog emphasizes its vital impact on the state's digital infrastructure, data security, and operational resiliency through various services. Key areas of influence include:

1. **Infrastructure security**: OCS protects state networks through a multi-layered approach, integrating tools like the Albert sensor, Extended Detection and Response (XDR) suite, and Intrusion Detection and Prevention Systems (IDS/IPS). These components collectively prevent unauthorized access, detect threats in real-time, and ensure robust responses to evolving cyber threats.
2. **Data Protection**: Leveraging encryption, multi-factor authentication, and Web Application Firewalls (WAF), OCS ensures data confidentiality and integrity. The Vulnerability Management Program proactively identifies and remediates weaknesses, reducing potential data breaches or other attacks on critical state data assets.
3. **Security Operations Center (SOC)**: The SOC provides 24/7 real-time monitoring and response, which allows for immediate action against incidents. With a defense-in- depth strategy, it not only addresses threats in real-time but also performs vulnerability scans and incident response tabletop exercises to build agency preparedness.
4. **Incident Response and Resilience**: The Critical Cyber Incident Response Team (CCIRT) and Managed Detection and Response (MDR) services enable rapid threat containment, investigation, and recovery. This proactive stance minimizes disruptions to state services and restores normalcy quickly, reinforcing public trust in government resilience.
5. **Risk Management and Compliance**: Through risk assessments, continuous monitoring, and alignment with frameworks like NIST CSF and CIS Controls, OCS establishes a strong compliance foundation, helping agencies manage both external and internal risks effectively. This includes structured risk management protocols and compliance reporting via Security Information and Event Monitoring (SIEM) tools.
6. **Service Management and Architecture Consulting**: OCS's consulting services in security architecture provide expert guidance to agencies, enabling them to implement strong security frameworks. Service management offerings further ensure that agencies have access to ongoing

monitoring, program oversight, and tailored security advice, supporting long-term cybersecurity stability.

7. **Awareness and Education**: Cybersecurity awareness training and practitioner education programs are critical for a security-first culture. By educating employees on cyber hygiene and providing structured training to cybersecurity professionals, OCS builds a knowledgeable workforce that can proactively identify and mitigate potential threats.

OCS's efforts highlight a comprehensive approach to cybersecurity, not only focusing on immediate responses to threats but also on long-term strategic planning and resilience- building across state agencies.

The updated catalog ensures transparency and accountability in the state's enterprise cybersecurity efforts.

Office of Cybersecurity (OCS) enterprise programs and services

OCS provides services to protect the state's digital infrastructure. The services described in the remainder of this document help protect state agencies' digital assets, reduce cyber risk, ensure compliance, and maintain public trust.

Enterprise IT security programs

OCS implements a robust, multi-faceted IT security strategy to protect state operations and data. This approach includes enterprise-wide IT security programs aligned with established frameworks. This coordinated effort enables Washington to maintain a resilient, secure digital environment that supports public trust and effective governance.

Enterprise IT security strategic planning

Enterprise IT security strategic planning is a critical initiative to safeguard the information and systems supporting state government operations. In an increasingly digital world, protecting sensitive data and ensuring the integrity of state operations is more important than ever. This strategic planning process provides a long-term roadmap for managing cybersecurity risks, responding to threats, and maintaining public trust.

The statewide IT security strategic plan establishes clear priorities and goals to protect the state's digital infrastructure. It requires collaboration across agencies, each contributing to the security of data and systems. The plan is designed to be adaptable, recognizing the ever-evolving nature of cybersecurity threats.

By implementing a comprehensive enterprise IT security strategic plan, the state can protect its digital assets, ensure continuity of operations, and reinforce public

trust. This proactive approach is essential in addressing the persistent and growing threat of cyberattacks and minimizing the potential impact of such attacks on state systems.

This plan goes beyond technology, emphasizing the integration of people, processes, technology, and policies to create a secure environment for state operations. It is a crucial element of modern governance, ensuring the state can serve its citizens effectively and securely in an increasingly digital world.

State information security policy and standard development

In today's digital world, where sensitive data is constantly at risk, protecting information assets is essential for organizations of all sizes - including state governments. One key approach to achieving this is by aligning information security frameworks. But what exactly does this mean, and how does it play into developing state information security policies and standards?

An information security framework is a structured set of guidelines, policies, and best practices designed to help organizations manage cybersecurity risks, mitigate threats, and respond to incidents.

Common frameworks include ISO/IEC 27001, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), Center for Internet Security (CIS) controls, NIST 800-53, and COBIT, each offering different approaches tailored to varying industries and needs.

Framework alignment involves ensuring that an organization's security policies and practices are consistent with the chosen framework. WaTech's Office of Cybersecurity has aligned with the NIST CSF and CIS Controls. Aligning with these frameworks involves implementing their specific requirements, such as conducting regular risk assessments, establishing a clear security policy, and continuously monitoring and improving security practices.

WaTech's information security policies are formal documents that outline how state agencies protect their digital assets, which include citizens' personal information and the state's data and IT infrastructure. Security standards, on the other hand, define specific, measurable requirements to implement these policies. These standards ensure that the state's IT infrastructure, processes, and practices are aligned with broader security frameworks, promoting consistency and effectiveness in preventing unauthorized access and cyber threats.

Developing these policies and standards is a collaborative effort that involves engaging cybersecurity experts, IT professionals, legal advisors, business leaders, and state agency representatives. The process begins with a comprehensive assessment of the current risks and vulnerabilities, followed by drafting security policies and standards that set clear objectives for information security. Each policy and standard sets clear, achievable objectives for information security and

outlines the specific measures to be taken to meet these objectives. After multiple reviews by subject matter experts, the final documents are reviewed and approved by multiple state governance bodies and formally adopted by the Technology Services Board (TSB). This approval process ensures transparency and public trust.

Given the constantly evolving cyber threat landscape, these policies and standards require regular reviews and updates to remain effective and relevant. Ongoing training and awareness ensure that all state employees understand their responsibilities in maintaining security, reinforcing the alignment with NIST CSF and CIS Controls.

In summary, the development and alignment of the state's information security policies and standards provide a robust defense against cyber threats. By adhering to well-established frameworks like NIST CSF and CIS Controls, the state can protect its digital infrastructure, maintain operation continuity, and safeguard citizens' personal information.

Cybersecurity awareness training

Organizations must ensure that all employees can recognize and mitigate potential cyber risks. A cybersecurity awareness training program offers a structured approach to educating staff on cyber threats, including phishing, malware, vulnerabilities, and data breaches. The goal is to foster a security culture by empowering everyone, from executives to entry-level staff, to protect sensitive data and follow best practices.

The Office of Cybersecurity (OCS) provides the state with a comprehensive cybersecurity awareness training program that manages everything from design to execution, including refreshed content and ongoing support. Here's how the service works:

1. **Assessment:** The program starts with an evaluation of the state's existing cybersecurity practices and employee needs to tailor training to relevant threats.
2. **Training program development:** Based on the assessment, OCS designs a training program that includes interactive modules, videos, quizzes, and workshops. The content is engaging and accessible to employees regardless of their technical background.
3. **Implementation:** In partnership with the Department of Enterprise Services (DES) and agency training coordinators, OCS deploys the program across the state via the Enterprise Learning Center platform, allowing employees to complete training at their own pace.
4. **Refreshed content and ongoing support:** As cyber threats evolve; OCS continually updates the program with new content to keep employees informed about the latest threats. Ongoing support is provided to answer

questions and offer additional resources.

5. **Monitoring and reporting:** OCS tracks employee progress and participation, generating reports that help agencies evaluate the program's effectiveness and identify areas for improvement.

Cybersecurity is everyone's responsibility – not just the IT departments. A well-executed cybersecurity awareness training program helps reduce the risk of cyberattacks by ensuring employees understand potential threats and know how to respond appropriately.

Cybersecurity practitioner education

With the increasing complexity of cyber threats, Washington state requires skilled professionals to safeguard its data and IT infrastructure. To meet this demand, the Office of Cybersecurity (OCS) offers cybersecurity practitioner training programs to equip the state's workforce with the necessary skills to defend against cyberattacks.

This training program provides a structured education in cybersecurity, teaching participants how to identify, prevent, and respond to various threats. The program caters to a wide range of learners, from beginners entering cybersecurity to experienced IT professionals looking to enhance their cybersecurity expertise.

This training is an excellent opportunity for individuals to enter a fast-growing and rewarding career field. It provides the foundational and advanced knowledge required to succeed as a cybersecurity professional, preparing them to meet the industry's evolving demands.

Enterprise cyber risk management

An enterprise cyber risk management program is a strategic framework to protect an agency's data and IT infrastructure from cyber threats. This comprehensive approach helps agencies identify, assess, and manage risks, ensuring business continuity and minimizing potential cyberattack damage.

At its core, a risk management program involves a proactive series of measures, identifying threats, system vulnerability assessments, and implementing security controls to prevent cyberattacks. Continuous monitoring of the digital environment is also crucial, enabling real- time detection and response to emerging threats.

The program begins with a risk assessment, evaluating the state's digital assets to determine which are critical to operations. This risk assessment includes identifying potential cyber threats and evaluating their potential impact on the organization.

After risks are identified, the risk management plan is developed and implemented. This plan details the actions necessary to mitigate identified risks, such as strengthening defenses, improving system configurations, and enhancing incident response capabilities.

The program's success relies on continuous monitoring and updating. As the cyber threat landscape evolves, the program must adapt, with regular reviews to address new vulnerabilities and emerging risks. This flexibility ensures that agencies remain protected against the latest cyber threats.

In addition to defending against external threats, the risk management program addresses internal risks, such as unauthorized access to sensitive data by employees or contractors.
Access controls, regular audits, and robust data management policies help minimize these risks.

Security Operations Center ("The SOC")

The Security Operations Center (SOC) is a team within the Office of Cybersecurity (OCS) that works around the clock to protect the state's digital systems. Using a "defense-in-depth" strategy, the SOC layers multiple security tools and techniques to secure networks and data. The team can detect, analyze, and respond to cybersecurity threats quickly and effectively.

During a cyber incident, the SOC promptly notifies the relevant people, aids in containment and eradication, collaborates with teams to recover services, and ensures a swift return to normalcy. The SOC also works to prevent future threats by conducting regular security checks, managing weaknesses, and following security rules and best practices.

The SOC's work is divided into three main service areas: *Incident response services, security infrastructure services, and service management*.

Enterprise incident response services

Incident response services provide comprehensive support to agencies facing various cyber threats in the event of an agency or enterprise-level incident. These services are designed to help agencies detect, respond to and recover from incidents, ensuring minimal disruption to operations. Incident response services include specialized teams and tools that work together to address threats, improve readiness, and strengthen security.

Here is a breakdown of the incident response services offered by OCS:

Critical Cyber Incident Response Team (CCIRT)

The Critical Cyber Incident Response Team (CCIRT) responds quickly to serious cybersecurity threats, like data breaches, ransomware, and other attacks that can disrupt services. When an incident occurs, CCIRT identifies the issue, contains the threat, investigates the cause, and minimizes damage. The team also keeps leaders and staff informed throughout the process.

CCIRT's key tasks include:

- Detecting threats: Quickly identifying the issue.
- Containing threats: Stopping the spread of damage.
- Investigating: Understanding what caused the incident and what was affected.
- Responding: Removing harmful software and fixing security gaps.
- Recovery: Restoring services and improving defenses to prevent future issues.

This service helps agencies respond swiftly and recover from incidents, ensuring critical operations continue with minimal disruption.

Tabletop exercises

Tabletop exercises help agencies prepare for cybersecurity incidents by simulating real- world attack scenarios. These exercises involve gathering key staff to walk through how they would respond to various types of threats, such as data breaches or ransomware attacks, in a controlled environment. The goal is to test the readiness of response plans, improve communication, and identify any procedural gaps. This service helps ensure that teams are well-prepared to handle incidents effectively, minimizing downtime and reducing the risk of damage when a real cyber event occurs.

Dynamic Web Application Vulnerability Scans

Dynamic Web Application Vulnerability Scans go deeper by testing interactive web applications' security, such as login pages or online forms. These scans simulate real-world attack methods, like trying to inject harmful code or exploit input fields. Proactively probing the application's functionality, they help identify more complex vulnerabilities such as SQL injection or cross-site scripting (XSS). This service is essential for web applications that process sensitive data or have dynamic features, ensuring that hidden weaknesses are found and fixed.

Security infrastructure services

These services protect against a wide range of cyber threats, keeping physical and digital assets safe. Security infrastructure services include many different technologies, tools, and processes that work together to secure an organization's IT environment. This covers everything from antimalware software to more advanced systems like intrusion detection, encryption, and multi-factor authentication. These services are important for stopping unauthorized access, finding potential threats, and responding to security problems as they happen.

Here is a breakdown of the security infrastructure services offered by OCS:

Albert sensor

Albert sensors are security tools given to U.S. state and local governments by the Multi-State Information Sharing and Analysis Center (MS-ISAC). These sensors monitor government networks for suspicious activity and share information about

threats across government levels. This teamwork improves national cybersecurity and helps states stay ahead of potential attacks.

Extended Detection Response (XDR) suite

The Extended Detection Response (XDR) suite is a comprehensive solution to enhance cybersecurity across an organization's digital environment. It integrates various security components to provide real-time threat detection, investigation, and response for endpoints, email applications, identities, and cloud services. Key features include:

- **Centralized threat detection:** Aggregates data from devices, emails, identities, and cloud environments to detect and respond to threats from a unified platform.
- **Automated investigations:** Uses security policies to analyze alerts, correlate them across the environment, and prioritize incidents for remediation.
- **Advanced threat protection:** Offers endpoint detection, network traffic analysis, and behavioral monitoring to identify complex attacks.
- **Simplified security management:** Provides a single console for managing security policies and incident responses.
- **Seamless integration:** Works with other security tools for coordinated threat intelligence and response.

The XDR suite enhances the state's ability to detect and respond to cyber threats efficiently, reducing risks and strengthening security.

Distributed Denial of Service (DDoS) prevention

DDoS prevention protects websites, networks, and services from being overloaded by malicious traffic. During a DDoS attack, many compromised devices flood a target with data, causing disruptions. DDoS protection finds and filters harmful traffic, blocking or redirecting it so services continue running. This protection is key for ensuring websites stay available to users and maintaining customer trust.

Intrusion Detection and Prevention Systems (IDS/IPS)

These are tools to protect networks from unauthorized access and harmful activities. An IDS watches network traffic for unusual patterns, like failed logins or spikes in activity, and alerts administrators if something seems abnormal. An IPS does the same but blocks threats in real-time. IDS provides alerts for manual response, while IPS offers automatic protection, working together to create a strong defense against cyber threats.

Web Application Firewall (WAF)

A Web Application Firewall (WAF) is a security tool that acts as a shield between a website and the internet. It filters and watches incoming traffic to stop cyber

threats. Unlike regular firewalls, WAFs protect web applications from attacks like SQL injection and cross-site scripting (XSS). They block suspicious actions immediately and can be customized to fit the specific needs of a website. This helps keep websites secure and prevents data breaches or downtime.

Service management

Service management ensures state agencies have the tools and support to keep their systems and data safe. It provides ongoing oversight and coordination of essential cybersecurity services, helping agencies identify and respond to potential threats. Service management helps agencies protect sensitive information, comply with regulations, and minimize risks by monitoring systems, managing security programs, and offering expert guidance. It is a key partner in maintaining a secure and resilient digital environment across the state.

Here is a breakdown of the SOC's Service management offerings:

Web Vulnerability Scanning

Web Vulnerability Scanning is a security service that tests a website for general weaknesses that attackers could exploit. This includes looking for outdated software, weak passwords, or misconfigurations that might leave the site vulnerable. These scans help agencies identify and fix common security issues before they can be used by cyber attackers. It is a proactive measure designed to ensure that websites are secure and less likely to be targeted in an attack.

Managed Detection and Response (MDR)

Managed Detection and Response (MDR) is a proactive cybersecurity service that protects state agencies from emerging threats. It combines advanced technology with expert oversight to detect and respond to security breaches before they cause harm.

MDR continuously monitors the state's digital ecosystem, analyzing data in real-time for signs of malware, ransomware, phishing, and other threats. Cybersecurity experts investigate and respond swiftly when suspicious activity is detected, tailoring actions to neutralize the threat with minimal disruption. Additionally, MDR offers ongoing security improvements, working with agencies to refine detection methods and provide insights to prevent future attacks.

Security Information Event Monitoring (SIEM)

Security Information and Event Monitoring (SIEM) is a key technology OCS uses to protect the state's digital environment. It gathers and analyzes real-time data from servers, networks, applications, and security devices to detect potential security incidents. Key features include:

- **Data aggregation:** Collects data from multiple sources for a complete view of security.

- **Correlation:** Links seemingly unrelated events, such as failed logins followed by unusual downloads, to identify threats.
- **Real-time monitoring:** Instant alerts for suspicious activity, enabling rapid response.
- **Incident response:** Automated responses to contain detected threats immediately.
- **Compliance reporting:** Generates reports to meet compliance requirements.

SIEM offers a proactive security approach, filling the gap left by traditional security measures like firewalls and antivirus programs. Continuously monitoring and analyzing security data helps detect and respond to threats before they cause damage.

Vulnerability Management Program (VMP)

The state's enterprise VMP is a key cybersecurity strategy to identify, assess, prioritize, and mitigate IT system weaknesses. Like regular health checkups, it continuously monitors the digital infrastructure to catch and fix security gaps before cybercriminals exploit them.

The process involves testing networks, applications, and devices for vulnerabilities, such as outdated software or misconfigurations. High-risk issues are addressed immediately, while lower-risk ones are tracked over time.

This program protects sensitive data, ensures regulatory compliance, and reduces the likelihood of costly cyberattacks, allowing agencies to stay ahead in an evolving digital landscape.

Security Design Review (SDR)

A security design review is a process used to evaluate the security aspects of a system or application before it's fully built or deployed.

During a security design review, experts closely examine the architecture and components of a system to identify any weaknesses or vulnerabilities. This includes looking at how data is protected, how users are authenticated, and how the system responds to potential threats. The goal is to catch and fix security issues early rather than after the system is already in use, which can be much more costly and damaging.

Security design reviews are essential for ensuring systems are built with security in mind from the ground up. They help avoid potential risks, protect sensitive data, and comply with industry regulations. Integrating security considerations into the design phase results in stronger, more resilient systems that are better equipped to withstand cyberattacks. In essence, a security design review is a proactive step in safeguarding digital assets, ensuring that security is not an afterthought but a

foundational aspect of the system's design.

Information security architecture and consulting

Information security architecture and consulting services help agencies protect their digital assets by designing and implementing strong security frameworks. These services provide the blueprint and expert guidance to build a secure and resilient digital fortress around sensitive information.

Information security architecture involves creating a comprehensive plan that outlines how different security measures, like firewalls, encryption, and access controls, fit together to protect data. This architecture is tailored to meet the business's specific needs, addressing all potential vulnerabilities.

Consulting services complement this by providing expert advice and guidance on implementing and maintaining these security measures. Architects work closely with agencies to assess their security posture, identify risks, and recommend strategies to strengthen their defenses. They stay up to date with the latest threats and technologies, ensuring the security architecture is robust and capable of adapting to new challenges.

Information security architecture and consulting services help protect data from cyber threats, comply with regulatory requirements, and build trust with customers and partners. By combining expert planning with ongoing support, these services ensure that an organization's digital assets are well-guarded against evolving cyber risks.

Security configuration approvals

Security configuration approvals are crucial to maintaining a safe and secure digital environment. They involve a process whereby any changes to the security settings of systems, applications, or network components must be reviewed and approved before implementation. This ensures that all modifications align with security policies and do not introduce vulnerabilities.

This process typically involves multiple steps, including submitting a change request, review of the request by security experts, and finally, approving or rejecting the change based on assessing the risk of its potential impact. It ensures that only well-considered, safe changes are made, preventing accidental exposure to cyber threats.

Security configuration approvals help maintain strong defenses against cyberattacks. By systematically controlling changes to security settings, organizations can reduce the risk of unauthorized access, data breaches, and other security incidents. This process protects sensitive information and ensures compliance with industry best practices and standards.

Information technology audit facilitation

Information technology (IT) audit facilitation is a service limited to WaTech and its hosted agencies that helps them prepare for and smoothly navigate through an IT audit. An IT audit thoroughly examines an agency's technology systems and practices to ensure they comply with regulatory standards, are secure, and function as intended.

IT audit facilitation involves gathering necessary documents, ensuring systems are in good shape, and addressing potential issues beforehand.

The facilitator works closely with the agency and the auditors, acting as a bridge to ensure clear communication and smooth processes. They help identify areas needing attention, guide the agency in implementing corrective actions, and ensure everything is well- documented.

By doing this, IT audit facilitation helps reduce the stress and confusion that can come with an audit. It ensures that the organization is well-prepared, reducing the risk of negative findings and helping to achieve a successful audit outcome.

Contact

Questions regarding this Service Catalog can be directed to Ralph Johnson, State Chief Information Security Officer (ralph.johnson@watech.wa.gov).