Cybersecurity Service

The Office of Cybersecurity (OCS), established under RCW 43.105.450, provides comprehensive cybersecurity services to all state agencies, emphasizing real-time threat detection and incident response to enhance cyber resilience. A 24/7 Security Operations Center (SOC) ensures continuous monitoring and rapid response to cyber threats, while incident response protocols and resilience planning support swift recovery. In addition, OCS collaborates with federal, state, local, and military partners to protect Washington's critical infrastructure and data assets.

Helpful information

Service availability
24/7/365

Planned maintenance
Performed as required during non-peak hours.

Related services

- Privacy

How to request service
Submit a request for service through our Customer Portal.

Service owner
Ralph Johnson
State Chief Information Security Officer

Intended customers

All state agencies.

Options available with this service

- To view the full range of services provided, visit the OCS Catalog of Services.

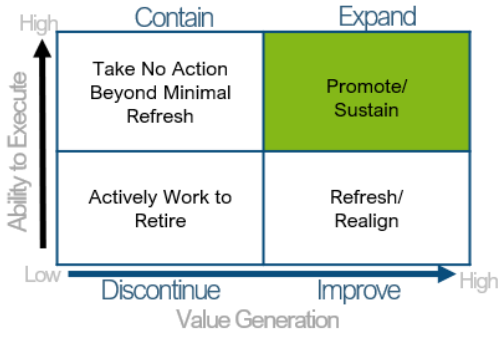
Customer engagement

- Monthly Enterprise Security Governance meetings and weekly CIO/CISO calls.
- OCS manages websites, Microsoft Teams, and channels for knowledge sharing and ad hoc engagements with state agencies.
- Monthly Technology Management Council.
- Open office hour sessions.

Action plan

Current activity

- Expand cybersecurity awareness and training.
- Strengthen incident response capabilities.
- Network Modernization with Secure Service Edge and Zero Trust.
- Improve risk management and compliance with SIEM and Vulnerability Management.
- Comprehensive cybersecurity metrics and AI-driven threat management.



One- to two-year goals

- Standardize KPIs across state agencies, deploy real-time dashboards for tracking incidents and compliance.
- Enhance cybersecurity workforce development – Partner with higher education, sponsoring cybersecurity certification programs and public-private partnerships.
- Enterprise-wide Zero Trust adoption – Implement a unified security framework that enforces continuous verification, least privilege access, and micro-segmentation.
- Statewide cybersecurity modernization and cloud security - Deploy Cloud Workload Protection Platforms to secure state-run multi-cloud and hybrid environments.

Three-to-five-year goals

- Fully implement Zero Trust Architecture in all state agencies by deploying adaptive Zero Trust Network Access solutions.
- Implement AI threat management across state agencies with behavioral anomaly detection, AI-driven SIEM for insider threats and automated threat intelligence.
- Improve cybersecurity workforce by offering competitive pay, effective hiring, and a modern work environment to retain talent in public service.
- Automate cybersecurity policy and compliance across state agencies and vendors by implementing real-time tracking, integrating enforcement.

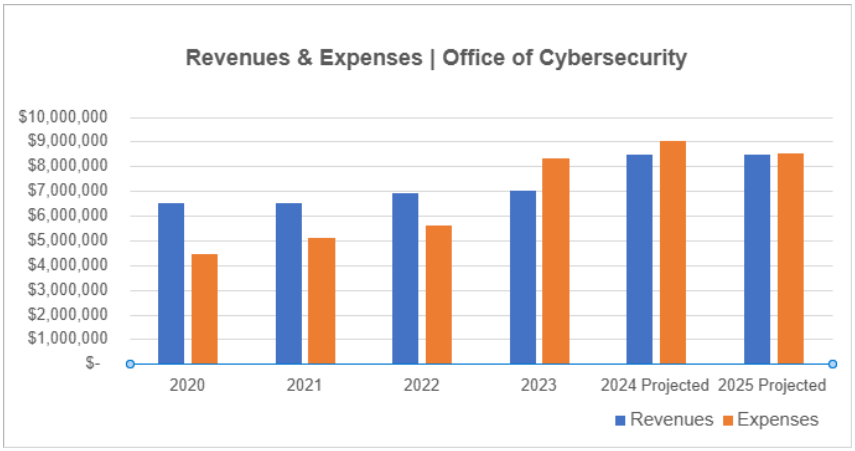
Service review and fully loaded service budget projection

Revenue source

The central service model funds the service under funding codes 3570 and 4672. The OCS central service model guarantees consistent funding for state government cybersecurity leadership and fosters collaboration with regional and national governments.

Profit/loss over time

As a service provider, WaTech OCS incurs both operating and staffing expenses. WaTech OCS generates revenue through allocations within the central service model. The accompanying graph compares OCS's revenue and expenses from 2020 to 2024 and projects the fiscal position for 2025.



For the fiscal years 2023 and 2024, expenditures surpassed revenue, which is anticipated to continue through 2025. The primary factors contributing to this deficit are increased costs associated with SIEM ingestion and MSSP services. To address this issue, OCS is reviewing all service offerings to assess their value and determine the feasibility of their continuation. Furthermore, OCS is implementing alternative log management platforms to enhance the efficiency of SIEM ingestion.