WaTech
Washington Technology Solutions

Technology Services Board

Security Subcommittee
August 8, 2024
9:00 am – 11:00 am

WaTech
Washington Technology Solutions

Today's Agenda

9:00 am	**Call to Order** • Reminder of Joint meeting • Welcome New Members	**Ralph Johnson**
9:10 am	**Subcommittee Charter Review *(Discussion)***	**Ralph Johnson**
9:25 am	**Policy & Standard Review**	
	• SEC-06-01-S Identification and Authentication	**Owner: Ralph Johnson** **SME: Kim Hort**
	• SEC-04-09-S Endpoint Detection and Response Standard • SEC-10 Incident Response Policy	**Owner: Ralph Johnson** **SME: Jack Potter**
9:35 am	**OCS Highlights: Security Operations *(Discussion)***	**Jack Potter**
9:50 am	**SLCGP Update *(Discussion)***	**Zack Hudgins**
10:00 am	**Enterprise Strategic Plan: Security Alignment**	**Ralph Johnson**
10:25 am	**Executive session: RCW 42.105.291(4)**	**Board Members**
10:50 am	**Public Comment**	
10:55 am	**Closing Remarks & Adjournment**	

Joint Meeting

RCW 43.105.291 (5) requires a joint meeting with Military Department EMD Cybersecurity Advisory Committee

Scheduled for September 26th

Preparation for the joint report to governor and appropriate committees of the legislature.

Report due annually each December 1st

WaTech
Washington Technology Solutions

Subcommittee Charter Review and Discussion

WaTech
Washington Technology Solutions

Policies & Standards Review

Identification and Authentication Standard

Purpose

Ensuring the appropriate controls for identifying and authenticating all organizational and non-organizational users and devices necessary to conduct state business.

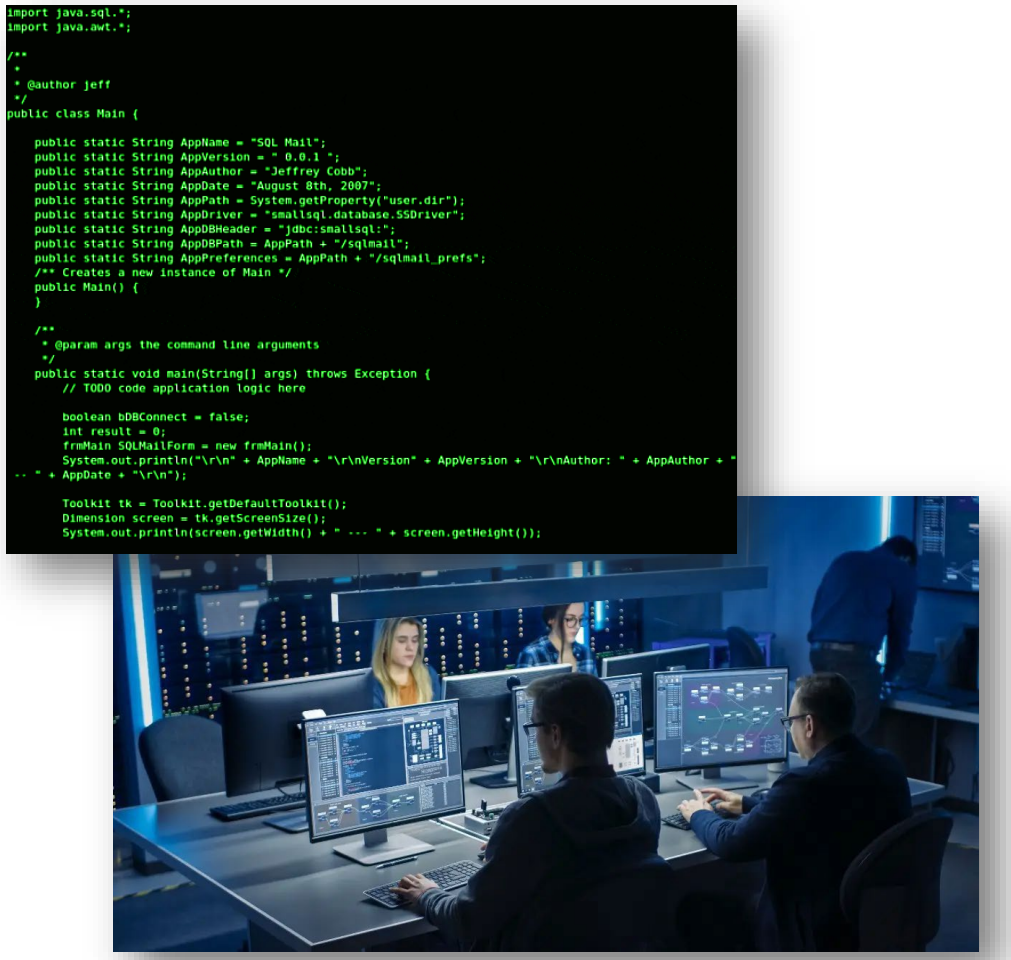
Objectives

- Align the processes and tools to link user and device identities to an account.
- Ensure authentication mechanisms are appropriate to the risk associated with the data category processed by the resource the user or device authenticates to.
- Requiring detailed documentation of authentication methods and processes in the annual application inventory and the agency's security program, ensuring transparency and compliance.
- Managing user, group, role, service, and device identifiers to ensure unique and secure access controls and prevent unauthorized access and privilege escalation.

WaTech
Washington Technology Solutions

OCS Highlights Security Operations

Security Operations aka “The SOC”

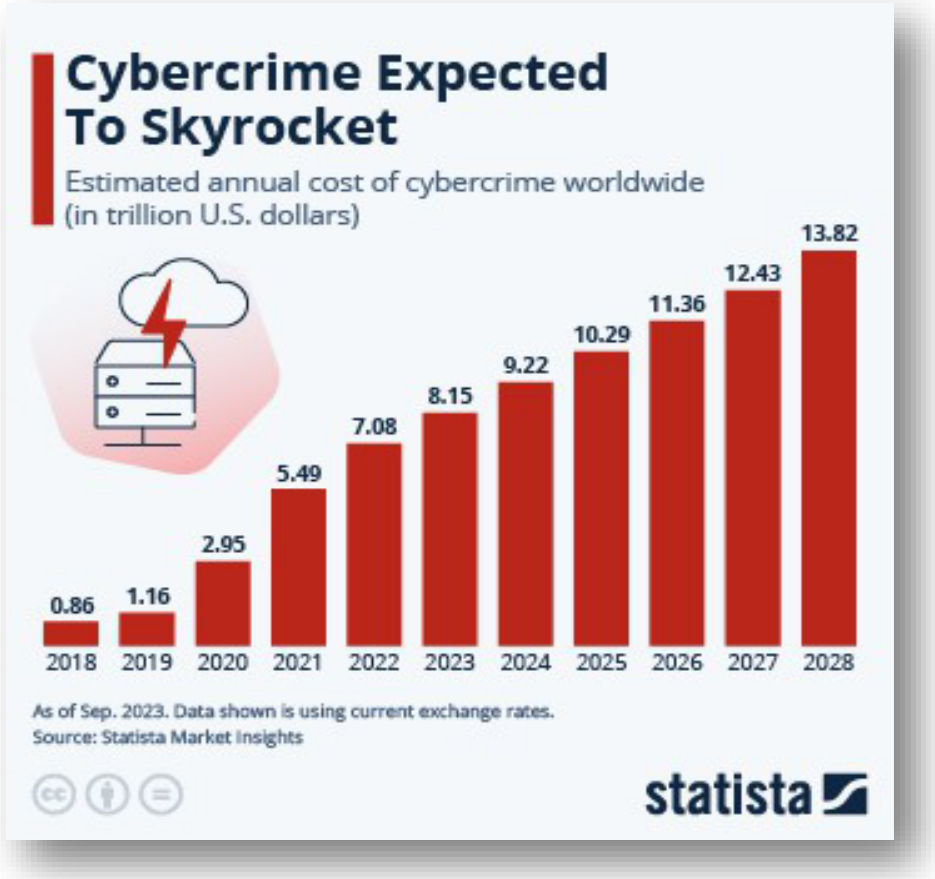


- To develop a centralized cybersecurity protocol.
- To detect and respond to security incidents.
- To create a model incident response plan.
- To provide formal guidance to agencies in:

  (III) Incident investigation & Response.
- To serve as a resource for local and municipal governments in Washington.
- To collaborate with state agencies.
- Other duties as assigned.

Common Threats We Face

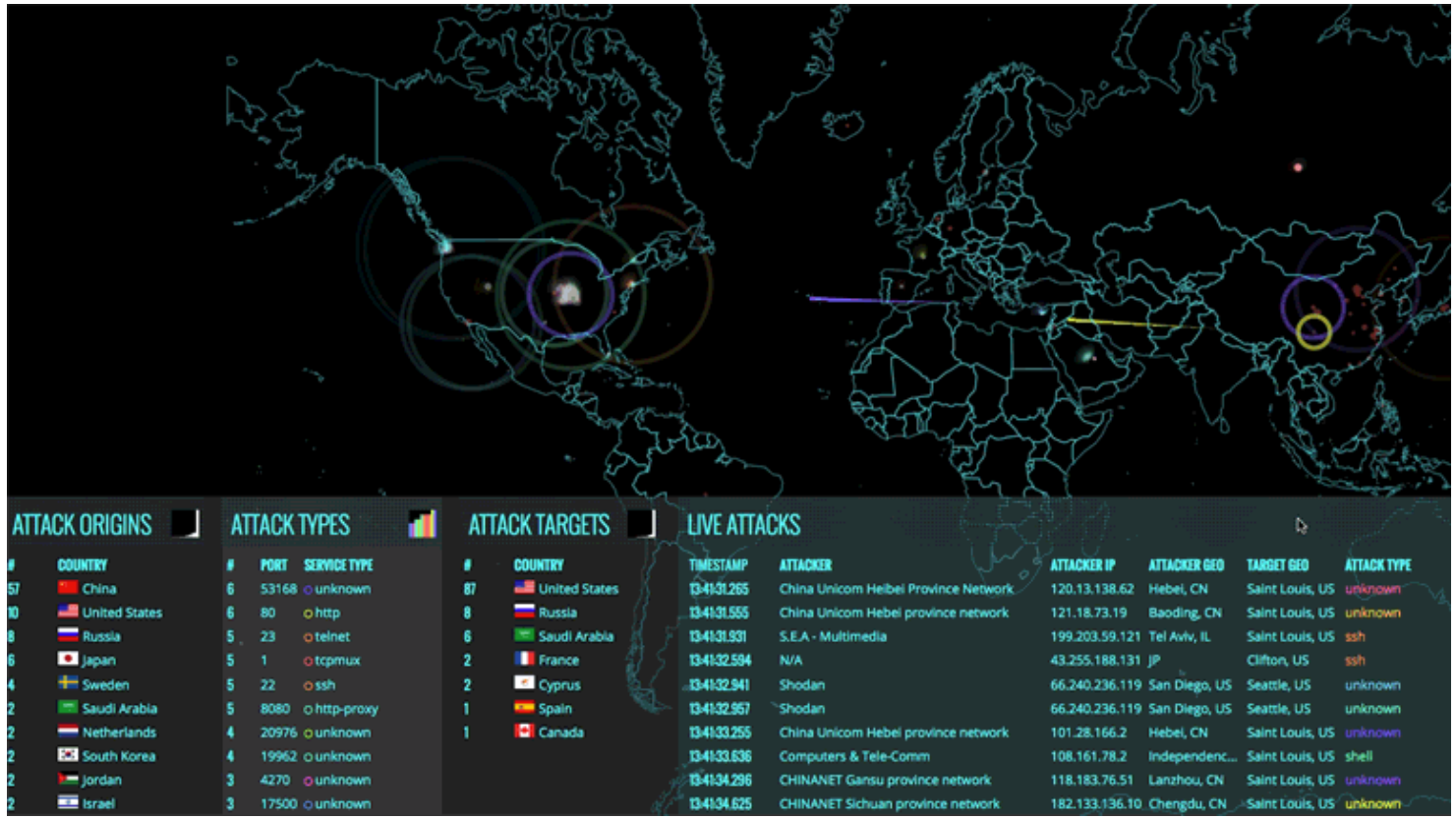
- Phishing attacks
- Vulnerabilities
- Malware
  - (Spyware, ransomware)
- Cloud security
- Multi-factor authentication (MFA)
  - (Enforcement/fatigue)
- AI advancing attacks



WaTech
Washington Technology Solutions

National Cyberthreats & Facts

- **353-million people** were impacted by data breaches in 2023.
- **343-million victims** were targeted in 2,365 cyberattacks in 2023.
- A data breach costs **$4.45 million** on average
- **Email is the most common vector for malware**, with around 35% of malware delivered via email in 2023.
- **94%** percent of organizations have reported email security incidents.
- 2023 saw a **72% increase in data breaches** since 2021 (which held the previous all-time record.)



Source: St. John, M. (2024) Cybersecurity Stats: Facts and Figures You Should Know. Forbes Advisor. Forbes.

The SOC- Teams

Security Infrastructure Team
"SOC"

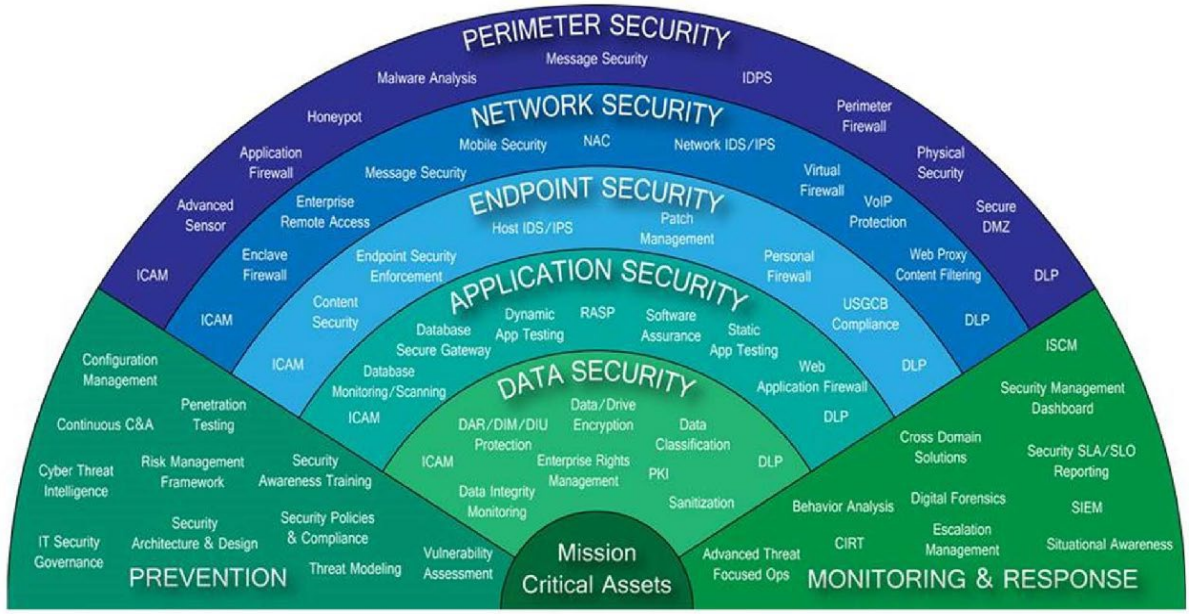
Threat Management

Critical Incident Response Team
"CIRT"

Security Infrastructure Defense in Depth

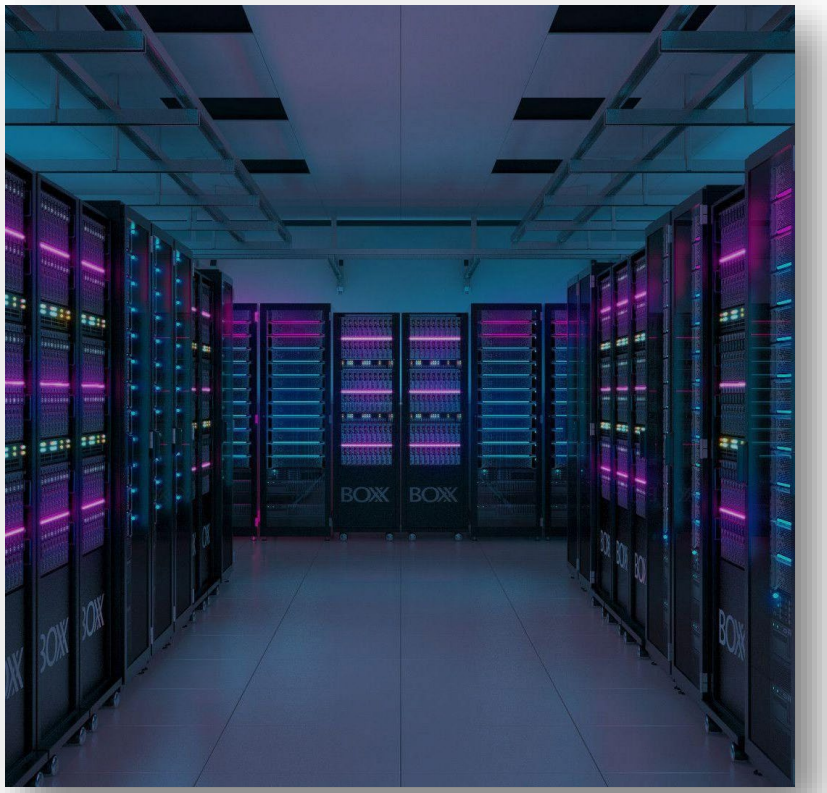
OCS uses multiple platforms including:

- Web Application Firewall (WAF)
- Distributed Denial of Service (DDOS)
- Intrusion Prevention System (IDS/IPS)
- Advanced Network Detection
- Endpoint Detection Response (EDR)
- Identity Management



Managed Detection Response (MDR)

- MDR monitors and escalates alerts to agency and enterprise staff for appropriate action.
- Automated response actions are currently in flight for assessment and implementation over the next quarter for both users and endpoints.
- Security Information and Event Management (SIEM)
  - This is used for rule detection and alerting across log analytics surfaces.



Security Incident Management

- OCS provides incident management for agencies, and for locals upon request.
- Escalation, forensics, guidance, support.
- Consists of detecting security incidents and assisting with remediation and recovery.
- Federal and 3rd party coordination e.g. - Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC).

WaTech
Washington Technology Solutions

Questions?

Find out more at the OCS website:
watech.wa.gov/cybersecurity

WaTech
Washington Technology Solutions

State Local Cybersecurity Grant Program (SLCGP)

SLCGP Update - Overview

- Federal four-year grant program targeted at Local, State and Tribal Governments to increase cybersecurity profiles.
- Part of the bi-partisan Infrastructure Investment Jobs Act (IIJA).
- Washington State received $17M over 4 years.

Discussion: FY 23 – Allowable Costs/ Allocations

- **Planning** - activities such as those associated with the development, review, and revision of the holistic, entity-wide cybersecurity plan and other planning activities that support the program goals and objectives.
- **Organization** - program management, structures and mechanisms for information sharing between the public and private sector, and operational support.
- **Equipment** - equipment used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.
- **Training** - establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies.
- **Exercises** - expenditures related to exercise scenarios testing identified cybersecurity risks and threats.
- **Management & Administration** - activities directly relating to the management and administration of SLCGP funds, such as financial management and monitoring (a maximum of up to 5% of the awarded funding).
- **Allocations** - 80% to Local Governments; 25% must go to Rural Local Governments.

SLCGP Update - Projects

- **Round One** - FY22 Award - 74 jurisdictions/entities, 93 projects
  - 24 agreements closed/projects complete
  - 50 agreements in progress
- FY23 Award – 29 jurisdictions/entities, 33 projects
  - 2 agreements closed/projects complete
  - 27 open
- **Round Two** - FY23 Recommended – 79 entities, 125 projects

SLCGP Update

In first two years:

- First Planning Committee meeting – November 2022.
- 252 projects funded in whole or part.
- $13M allocated to cybersecurity projects in state, local, Tribal governments.
- 26 projects completed.
- 143 applications year one.
- 189 applications year two.

- WaTech partnering with MIL/EMD to implement.
- Planning Committee has representatives from Local Governments, SOS, SAO, COM, MIL, WSP, WaTech, OSPI, GOV.

WaTech
Washington Technology Solutions

SLCGP Update – Round Two

- 189 applications received.
- Largest request was for more than $1.3M.
- Smallest request was for $1190.
- Project themes – training, planning, infrastructure, software tools, firewalls, monitoring, network updates, backup and recovery, MFA, testing, incident response plans, zero trust solutions, etc.

- More than **$17.3M** in requests for about **$5.3** available this year.
- Future year funding begins to diminish. This year two funding level was peak.
- Applications from Cities, Counties, Special purpose districts, educational districts, one Tribal government.
- **List of 79 entities, 125 projects approved by Planning Committee on Aug 6.**
- Next step is to notify entities and submit to FEMA/CISA for project approval.

SLCGP Update - Timeline

3/21	Send application to Planning Committee for review.
3/29	Send out solicitation for applications.
4/3	Presentation at Partners in Emergency Preparedness conference. *(Zack/Josh)*
4/8	Webinar.
4/17	Presentation at ACCIS conference. *(Melissa/Sierra)*
4/25	Webinar for Local Government.
5/10	Applications due.
5/11-6/7	EMD internal review *(rolling - send applications to scorers ¼ each week).*
6/10-7/12	Scoring Panel begins work.
8/6	Finalize awardees at Planning Committee meeting.
8/9	Send out announcements of funded/not funded projects.
7/15-8/15	Compile projects for FEMA/CISA review.
8/16	Send to FEMA for review.
8/16-9/13	Prep grant agreements.
9/16	*(tentative)* Funding released.
9/16-9/27	Send out grant agreements.

SLCGP Update - Questions

QUESTIONS? Please contact:

Zack Hudgins
Privacy Manager – WaTech
Zack.Hudgins@watech.wa.gov
Melissa Berry
SLCGP Program Manager - MIL/EMD
melissa.berry@mil.wa.gov
Sierra Wardell - MIL/EMD
Financial Operations Section Manager
sierra.wardell@mil.wa.gov

WaTech
Washington Technology Solutions

How Security Governance Aligns with the Enterprise IT Strategic Plan

Enterprise IT Strategic Plan 2023-2025

Connected Government, Stronger Communities, Better Washington

Goal #1
Create a Government Experience that Leaves No Community Behind

Goal Statement: Through a connected government that emphasizes service delivery and the experience of those we serve, we can achieve equitable outcomes across our communities.

Goal #2
Better Data, Better Decisions, Better Government, Better Washington

Goal Statement: Use data and insights to improve the experience of those we serve, prioritize service improvements, drive strategic decisions, and improve transparency.

Goal #3
Innovative Technology Solutions Create a Better Washington

Goal Statement: Prioritize solutions emphasizing access, technology, and innovation to address systemic societal challenges and align our decision-making for those we serve.

Goal #4
Transform How We Work. Best Workforce Ever.

Goal Statement: Attract and retain technology talent, advance our agencies' skill sets, instill an innovation culture, and establish new and agile processes and practices to achieve our future vision.

Our Pillars Digital Trust | Shared Governance | Equitable Outcomes | Service Excellence

Our Values Human-Centered | Inclusive Ideas | Courageous Innovation | Accessibility | Stay Nimble | Community + Connectivity

WaTech
Washington Technology Solutions

The Strategic Framework

Unifying Statement

Connected Government, Stronger Communities, Better Washington

Values

- Human-Centered
- Community + Connectivity
- Accessibility
- Courageous Innovation
- Inclusive Ideas
- Stay Nimble

Pillars

- Digital Trust
- Equitable Outcomes
- Shared Governance
- Service Excellence

WaTech
Washington Technology Solutions

Goal #1

Create a Government Experience that Leaves No Community Behind

Goal Statement: Through a connected government that emphasizes service delivery and the experience of those we serve, we can achieve equitable outcomes across our communities.

WaTech
Washington Technology Solutions

Goal #2

Better Data, Better Decisions, Better Government, Better Washington

Goal Statement: Use data and insights to improve the experience of those we serve, prioritize service improvements, drive strategic decisions, and improve transparency.

WaTech
Washington Technology Solutions

Goal #3

Innovative Technology Solutions Create a Better Washington

Goal Statement: Prioritize solutions emphasizing access, technology, and innovation to address systemic societal challenges and align our decision-making for those we serve.

WaTech
Washington Technology Solutions

Goal #4

Transform How We Work. Best Workforce Ever.

Goal Statement: Attract and retain technology talent, advance our agencies' skill sets, instill an innovation culture, and establish new and agile processes and practices to achieve our future vision.

Office of Cybersecurity

Vision

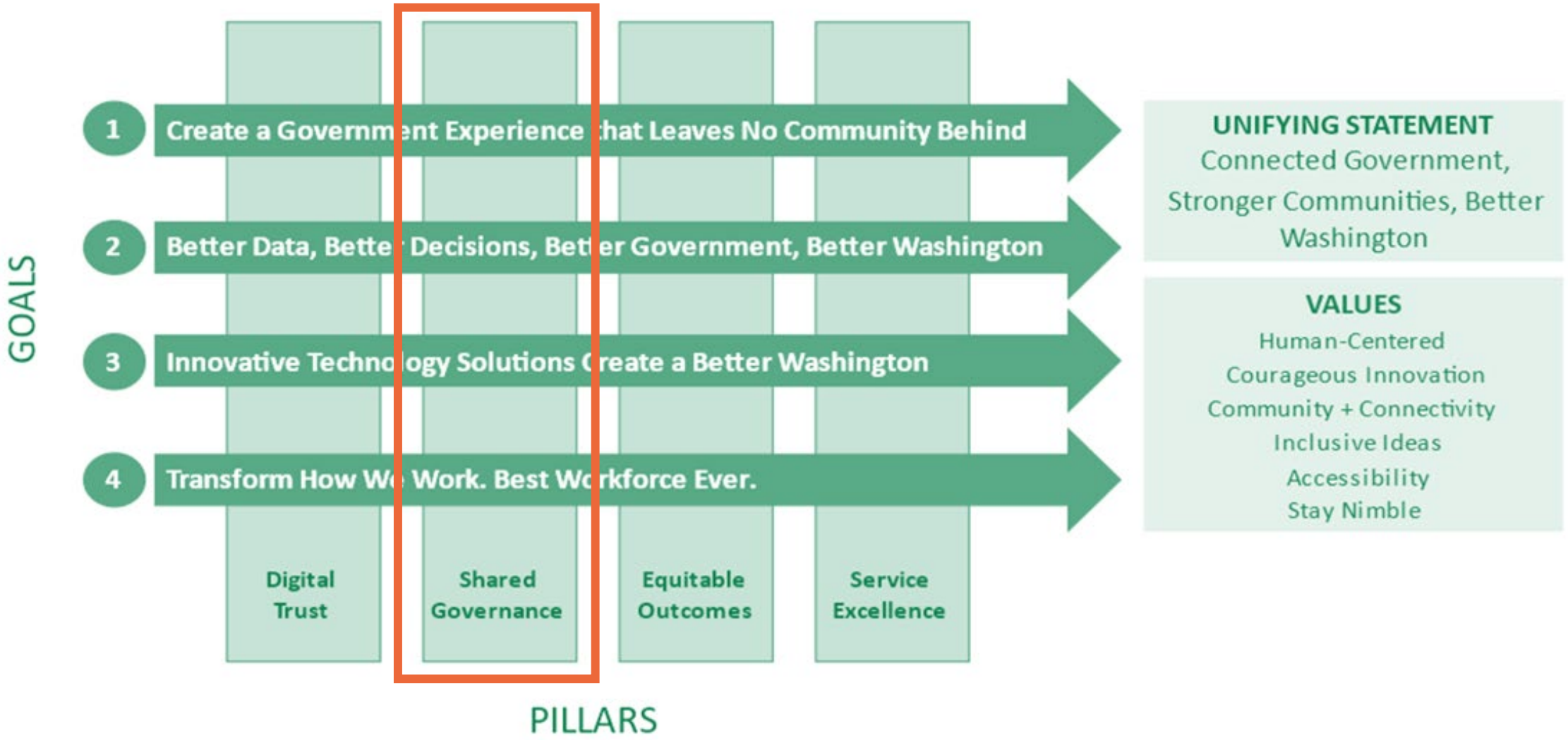
To make Washington State a national model for cybersecurity, building a secure digital environment that fosters a culture of security awareness, public trust, and supports the seamless operation of state services in a connected world.

Mission

The Office of Cybersecurity is dedicated to safeguarding Washington State's information assets through comprehensive standards, proactive measures, and services designed to minimize cyber-attack impacts and enable operational continuity.

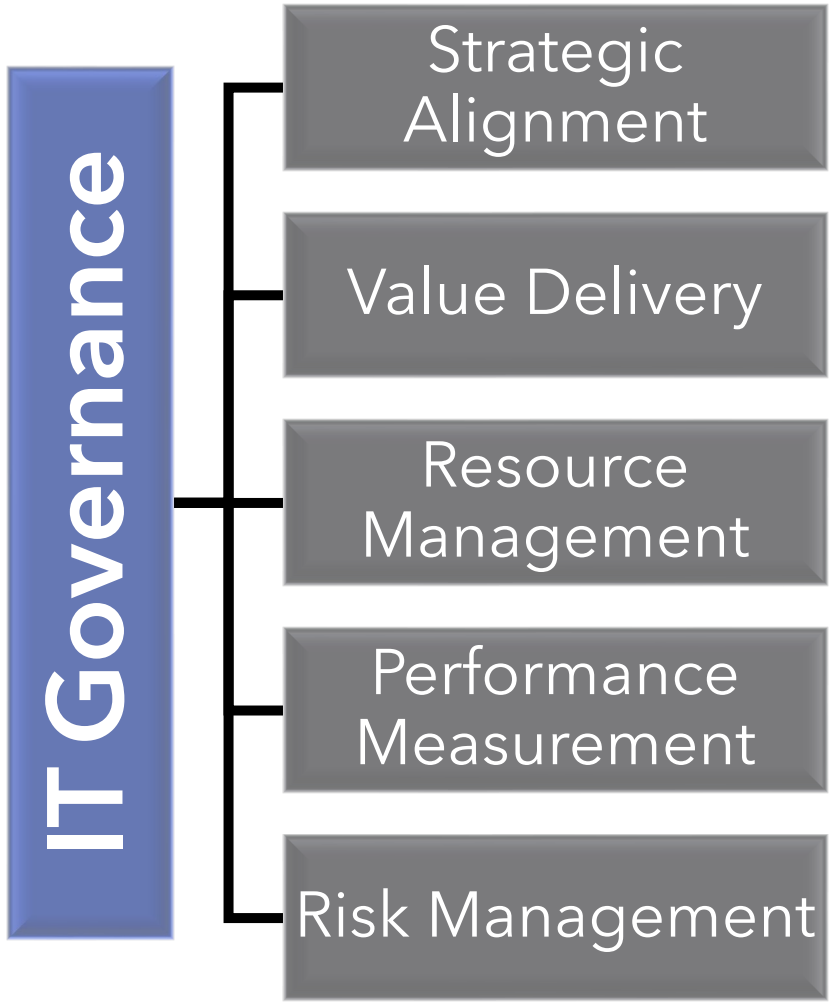
WaTech
Washington Technology Solutions

Putting it all together



Information Technology Governance

Actions an organization takes to ensure compliance with its information technology policies, standards, and procedures to meet business requirements.



WaTech
Washington Technology Solutions

Drivers for IT Governance

Putting it all together

Putting it all together

Digital trust refers to individuals, organizations, and societies' confidence in the reliability, integrity, and security of digital technologies, services, and platforms. In an increasingly digitalized world, where interactions, transactions, and communication are predominantly online, digital trust fosters collaboration, innovation, and economic growth.

WaTech
Washington Technology Solutions

Key Components


Security


Privacy


Transparency


Reliability


Accountability


Ethics and Integrity


User Empowerment

Putting it all together

Putting it all together

Service Excellence

Service excellence is a philosophy or approach that emphasizes providing exceptional service to customers or clients. It goes beyond simply meeting basic needs or expectations and aims to exceed them by delivering outstanding experiences that leave a lasting positive impression.

WaTech
Washington Technology Solutions

Key Aspects

Customer Focus

Quality Service Delivery

Continuous Improvement

Empowered Employees

Personalization

Positive Attitude and Culture

WaTech
Washington Technology Solutions

Executive Session

Executive Session in progress.

Resuming public meeting at 10:50 a.m.

WaTech
Washington Technology Solutions

Public Comment

WaTech
Washington Technology Solutions

Closing Remarks