WaTech
Washington Technology Solutions

Technology Services Board

Security Subcommittee Meeting
August 10, 2023
9:00 am – 11:00 am

WaTech
Washington Technology Solutions

Current TSB Members

Industry Members
Butch Leonardson – Retired CIO
Paul Moulton – Retired CIO
Tanya Kumar – Oracle

Legislative Members
Rep. Travis Couture – House R
Rep. Chipalo Street – House D
Sen. Matt Boehnke – Senate R
Sen. Joe Nguyen – Senate D

Executive Branch (Agency Directors)
Bill Kehoe – State CIO & Chair
David Danner – UTC
Cami Feek - ESD
Tracy Guerin – DRS

Other Government
Viggo Forde – Snohomish County
Andreas Bohman – UW-IT

Vacancies:
Labor Union Representative

Members present
Members absent

WaTech
Washington Technology Solutions

Agenda

TOPIC	LEAD	PURPOSE	TIME
Welcome | Agenda review | New members	Bill Kehoe	Introductory remarks	9:00 a.m.
Review and approve May 11 meeting minutes	Bill Kehoe	**Approval** of minutes	9:10 a.m.
Debrief on changes to this Subcommittee	Derek Puckett	Information	9:15 a.m.
Policies & Standards review: • Acceptable Use Policy • Change Management Policy • Configuration Management Standard • International Travel Security Policy & Standard • Vulnerability Management Standard	Bill Kehoe Stevens Fox Sam Zee	**Review and Recommend Approval** to full Board on 9/14	9:30 a.m.
State & Local Government Cybersecurity Grant Program	Zack Hudgins	Status/Board discussion	10:00 a.m.
Whole state approach to Cybersecurity	Ralph Johnson	Information	10:20 a.m.
Public comment			10:35 a.m.
Executive Session for members and select staff only – Closed to public	Bill Kehoe	Board discussion	10:40 a.m.

WaTech
Washington Technology Solutions

Review 5/11/23 Minutes

WaTech
Washington Technology Solutions

Debrief on Changes to this Subcommittee

Technology Services Board Security Subcommittee

Purpose: Provide advice, recommendations, and policy that strengthen cybersecurity in the state.

Membership: Comprised of a subset of members appointed to the board, as determined by the chair of the technology services board. The chair may make additional appointments to the technology services board security subcommittee to ensure that relevant technology sectors are represented.

Structure and collaboration:

- Created within the Technology Services Board as a subcommittee.
- Required to annually hold a joint meeting with the Cybersecurity Advisory Committee within the Emergency Management council.
- Jointly responsible to provide a state of cybersecurity report specifying recommendations considered necessary to address cybersecurity in the state.
- Responsible for coordinating the implementation of any recommendations in the above-mentioned report.

SSB 5518 – Creation of the Technology Services Board Security Subcommittee

Activities:

- Review emergent cyberattacks and threats to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies.
- Assess emerging risks to state agency information technology.
- Recommend a reporting and information sharing system to notify state agencies of new risks, risk treatment opportunities, and projected shortfalls.
- Recommend tabletop cybersecurity exercises, including data breach simulation exercises.
- Assist the office of cybersecurity in developing best practices recommendations for state agencies.
- Review the proposed policies and standards developed by the office of cybersecurity and recommend their approval to the full board.
- Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies.
- Assist in developing the annual state of cybersecurity report.

Cybersecurity Advisory Committee as a Subcommittee of the Emergency Management Council

Purpose: Provide advice and recommendations that strengthen cybersecurity in both industry and public sectors across all critical infrastructure sectors.

Membership: Organizations with expertise and responsibility for cybersecurity and incident response - local government, tribes, state agencies, institutions of higher education, the technology sector, and first responders.

Activities:

- Identify which local, tribal, and industry infrastructure sectors are at the greatest risk of cyberattacks and need the most enhanced cybersecurity measures.
- Use federal guidance to analyze categories of critical infrastructure in the state that could reasonably result in catastrophic consequences if unauthorized cyber access to the infrastructure occurred.
- Recommend cyber incident response exercises that relate to risk and risk mitigation in the water, transportation, communications, health care, elections, agriculture, energy, and higher education sectors.
- Partners with the TSB security subcommittee.

WaTech
Washington Technology Solutions

Security Policy and Standard Review

WaTech
Washington Technology Solutions

Acceptable Use Policy

WaTech
Washington Technology Solutions

Change Management Policy

Configuration Management Standard

WaTech
Washington Technology Solutions

International Travel Security Policy & Standard

WaTech
Washington Technology Solutions

Vulnerability Management Standard

WaTech
Washington Technology Solutions

State & Local Government Cybersecurity Grant Program Update

WaTech
Washington Technology Solutions

Cybersecurity Planning Committee

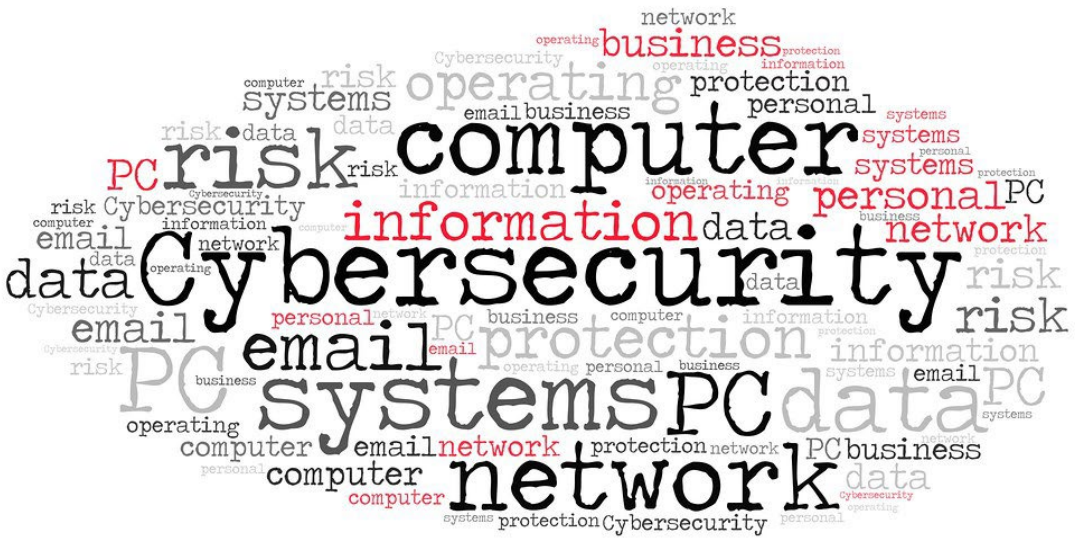
- Committee formed and meeting since November 2022.

Notice of Intent (NOI)

- Sent to local governments May 8, 2023.

Statewide Cybersecurity Plan

- Plan sent and approved by CISA/FEMA.

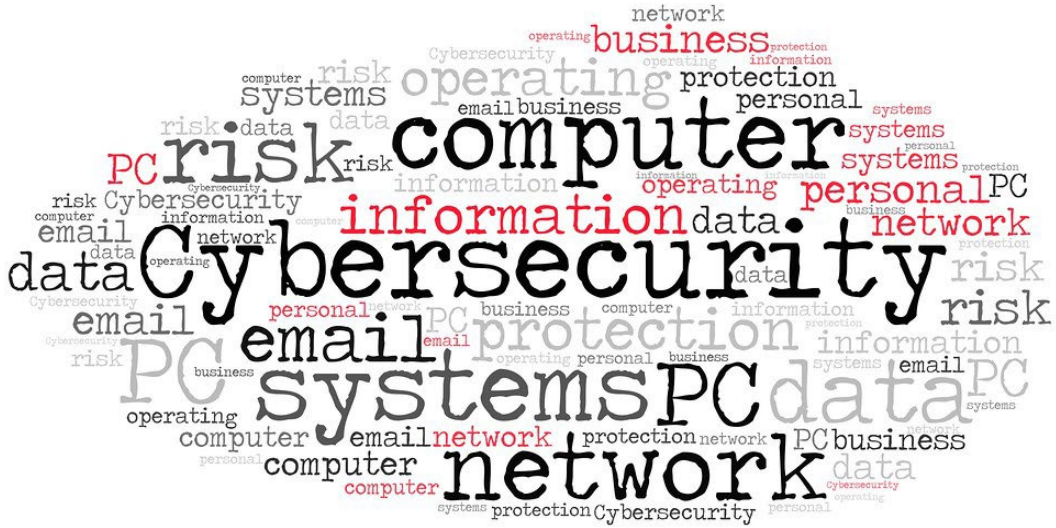


Application Review Process

- Planning Committee scores, ranks, and selects projects for funding.
- Package projects, re-submit projects to FEMA for approval.
- Planning Committee will rank and select projects for funding mid August.

Grant Applications

- Application submittal period ended July 18.
- 99 entities submitted 143 projects.
  - City: 57
  - County: 23
  - Tribal: 9
  - Special Purpose District: 18
  - School: 18
  - College: 15
  - State Agency: 3
- **Total funding requested: $15,478,157**
- Local-rural: $4,618,968
- Local-not rural: $8,650,563
- State: $2,208,626
- **Ineligible projects: 5**



SLCGP Project Types/Samples

- **Projects across all Objectives**
  - #1 Planning, program, governance
  - #2 Assessment, vulnerability scanning
  - #3 Solution implementation, close identified gaps
  - #4 Training

- **Types of projects**
  - Plan and policy development to include response and recovery
  - System testing and vulnerability assessment
  - Firewalls and security hardware
  - Monitoring and response systems
  - Identity management/MFA
  - Program development
  - Training to include certification of IT staff

WaTech
Washington Technology Solutions

“Whole of State” approach to Cybersecurity – Strategic Threat Intelligence Center (STIC)

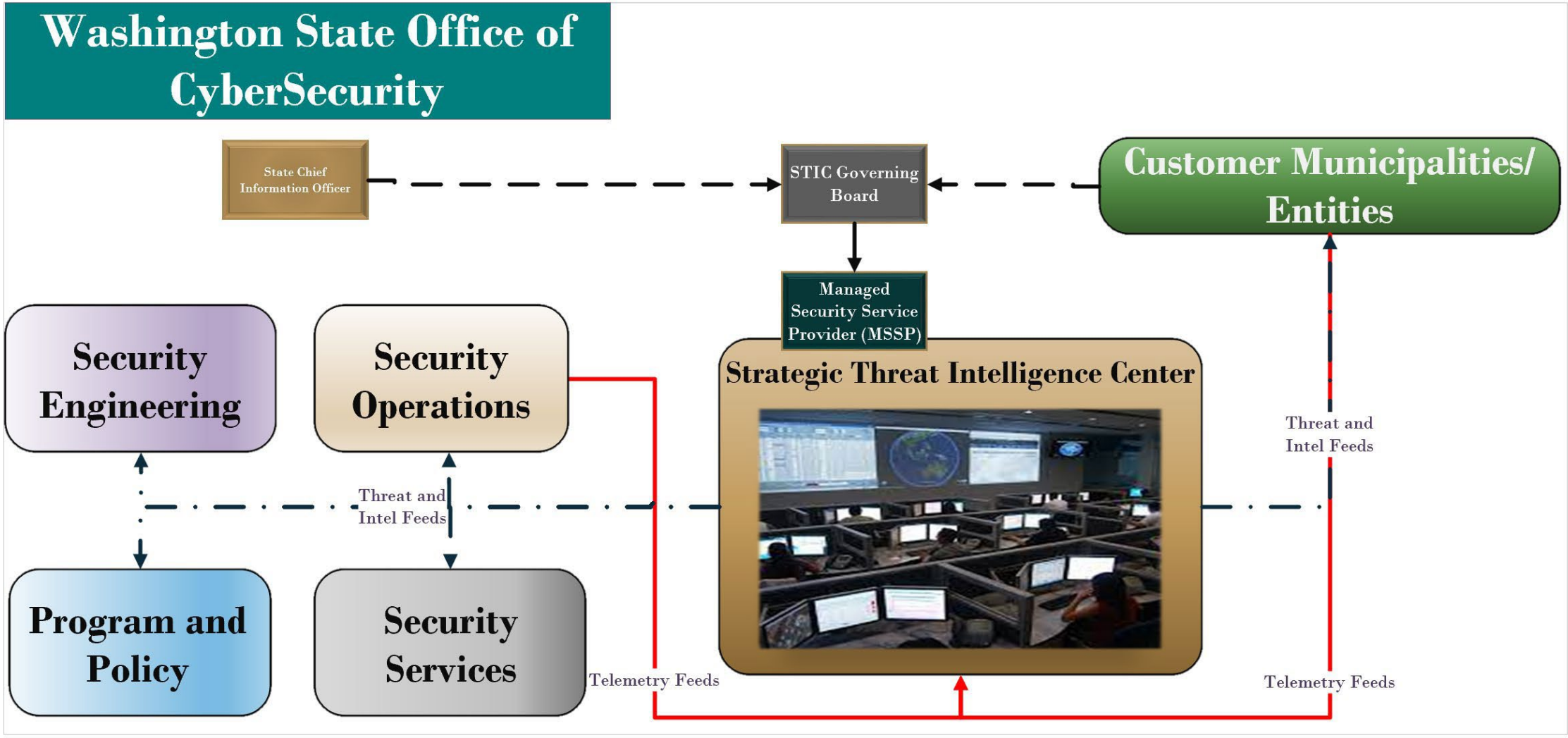
WaTech
Washington Technology Solutions

What is a Strategic Threat Intelligence Center?

A comprehensive range of services including:

- Comprised of skilled personnel
- Advanced facilities
- Monitoring systems
- Whole of State Threat visibility
- Whole of State Incident Response capabilities
- Resource sharing for digital security equity

Conceptual Strategic Threat Intelligence Center Architecture



WaTech
Washington Technology Solutions

46 Stakeholders

Representing 30 jurisdictions

Benton County
City of Bellevue
City of Everett
City of Kent
City of Kirkland
City of Lynnwood
City of Mill Creek
City of Renton
City of Seattle
City of Spokane
City of Tacoma
City of Vancouver
City of Walla Walla
Clark County PUD
Clark County
Walla Walla County
Cowlitz 911
Grant County PUD
King County
Kitsap County
Lewis County
Pierce County
Port of Tacoma
Snohomish County
Sound Transit
South King County Fire
University of Washington
Valley Communications WA
State Auditor (SAO)
Whatcom Transportation Authority

Benefits of a Strategic Threat Intelligence Center

- 24/7/365 monitoring, and event correlation;
- Incident response management;
- Device management and maintenance;
- Threat and vulnerability management;
- Compliance management;
- Malware and forensic analysis;
- Risk analytics and attack path modeling;
- Countermeasure implementation;
- Automated response and remediation prioritization;
- Penetration testing;
- Security awareness training.

Plan

- Initial Stakeholder conversations, planned future engagements
- Vision and Mission Definition and Project Charter
- Problem/Challenge Document
- Engage Consultant
- Challenge Procurement Process (not protracted RFP)
  - Define limitations (aka requirements)
  - Solicit challenge applications
  - Select MSSP(s) to meet the challenges

Operational within 6 Months of Contract Execution

Public comment

WaTech
Washington Technology Solutions

Executive Session – Closed to public