WaTech
Washington Technology Solutions

Technology Services Board (TSB)
Security Subcommittee Meeting Minutes

May 9, 2024
9:00 a.m. – 11:00 a.m.
Hybrid – 1500 Jefferson St SE, Olympia, WA; Presentation Room and Virtual via Zoom

---

Call to Order – Ralph Johnson

Chair Ralph Johnson, called the meeting to order at 9:00 am.

TSB Security Subcommittee Charter Review – Ralph Johnson

The discussion centered on the Security Subcommittee Charter, which aims to enhance the security posture of Washington state as outlined in RCW. The subcommittee's membership has been reconstituted, and the goal is for the Charter to be approved by the full Technology Services Board (TSB) in their June meeting. Once approved, the new membership will take effect, and meetings will continue to be scheduled quarterly. Additionally, there will be a joint meeting with the Emergency Management Division's Cybersecurity Advisory Board, as mandated by statute, and the Charter will be reviewed annually.

OCS Highlight: Policy & Program Management – Ralph Johnson

The Office of Cybersecurity (OCS) provides a monthly newsletter with updates and cybersecurity tips to CIOs and CISOs, who are encouraged to share it with their staff. This newsletter covers topics such as protecting Internet-connected devices, and OCS occasionally issues information security alerts about emerging issues like mobile device updates. OCS offers hosted learning sessions on cybersecurity for various groups, holds lunch and learn events, and organizes special events like Cybersecurity Awareness Month in October and Privacy Week in January. The policy and program management branch focuses on risk management, developing a risk assessment program for systems in production and building a risk register to report statewide risks. They are also creating a cybersecurity reference framework covering the entire IT stack and collaborating with national and local organizations for a comprehensive security approach.

SLCGP Grant Update – Zack Hudgins

Zack discussed the State Local Cyber Security Grant Program (SLCGP), emphasizing its importance in addressing cybersecurity needs for local governments. The federal program, part of the IIJA, allocates $1 billion over four years across 54 jurisdictions, with Washington State receiving approximately $17.6 million. The state legislature provided the necessary match funding, with 80% of the award going to local entities and 25% directed towards rural communities. The current year's

funding is about $5.3 million, with a May 10th deadline for applications. The program focuses on planning, organization, equipment, training, and exercises, with requirements for alignment with state or local cybersecurity plans.

Local & National Cybersecurity Coordination – Ralph Johnson

In WaTech and the Office of Cybersecurity (OCS), there was significant coordination with national and local cybersecurity organizations. They collaborated with the Cybersecurity and Infrastructure Security Agency (CISA), which provided various services like risk assessments and cyber hygiene evaluations. Additionally, they worked closely with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which helped share critical cybersecurity information and provided tools such as the Albert sensors for intrusion detection. The FBI and Secret Service also collaborated with WaTech, especially on major cybersecurity incidents. This robust network of partnerships enhanced the state's overall cybersecurity efforts.

Future Subcommittee Membership – Ralph Johnson

Ralph updated the Board on the status of the membership. The new membership is nearly complete, with 18 of the 19 members identified and 13 confirmed. The approval of the Charter by the TSB is still pending.

Scheduling: Joint Meeting with Cybersecurity Advisory Committee of the Emergency Management Council (2SSB 5518 - 2023) – Ralph Johnson

A joint meeting between this committee and the EMD Cybersecurity Advisory Committee is scheduled for September 26th, resulting in five meetings annually. The joint meeting aims to facilitate collaboration and improve the state's critical infrastructure cybersecurity posture.

Policy & Standard Review – Ralph Johnson

Ralph reviewed the following policy and standard:

The Access Control Policy, which replaces sections 6.1 and 6.2 of 141.10, has been updated to align with T853 and CIS controls, and integrates with the NIST Cybersecurity Framework. It requires management to handle user accounts and roles, with an emphasis on regular evaluation of entitlements and timely removal of accounts for individuals who have left the organization. The policy also enforces the principle of least privilege, ensuring that individuals only have access to the resources necessary for their work.

The Network Security Standard, replacing sections 5.15 and 5.4 of 141.10, establishes layered network security controls to safeguard data confidentiality, integrity, and availability. It aligns with industry standards such as NIST and others.

Both documents went through a standard approval process and were reviewed for consistency with current standards. A three-year review cycle is established for these documents, although updates may occur sooner if there are significant changes in industry standards. Additionally, updates will be

made to align with the new CSF 2.0 as administrative changes, without affecting the core content of the policies.

A poll was provided for members to vote and the vote was unanimous for both items to move forward to the TSB for approval.

10:30 am - Executive Session

An executive session was held for 20 minutes to discuss sensitive security topics and information pursuant to RCW 43.105.291(4). The session closed at 10:50 am; no action was taken.

Public Comment

No public comments were received.

The meeting was adjourned at 11:00 am.

Submitted by Leanne Woods, Board & Committee Program Administrator