WaTech
Washington Technology Solutions

Technology Services Board (TSB) Security Subcommittee Meeting Minutes

August 10, 2023
9:00 a.m. – 11:00 a.m.
Attendees: Bill Kehoe, Rep. Travis Couture, Paul Moulton, Andreas Bohman
Hybrid – 1500 Jefferson St SE, Olympia, WA; Presentation Room and Virtual via Zoom

Welcome, Agenda Review, New Members, 5/11/23 Minutes Review – Bill

Bill Kehoe, TSB Chair, welcomed new members to the meeting, including Representative Travis Couture and Andreas Bohman, CIO for the University of Washington. He then reviewed the agenda for the day and reviewed the May 11 meeting minutes. This subcommittee meeting is now open to the public.

Debrief on Changes to this Subcommittee – Derek

Derek Puckett, WaTech Legislative Director, briefed attendees on the changes introduced by Second Substitute Senate Bill 5518, which formalized the creation of the Technology Services Board Security Subcommittee. As defined by law, while the full TSB retains the ultimate authority, this subcommittee can make policy recommendations. It will also participate in an annual joint meeting with the Cybersecurity Advisory Committee from the Emergency Management Council (EMC) at the Washington Military Department (WMD) to enhance information sharing across state government and broader emergency management entities. The subcommittee is also mandated to produce an annual joint report on cybersecurity in coordination with EMC's Cybersecurity Advisory Committee. The first report is due Dec. 1, 2023.

Derek highlighted additional mandates of the bill, emphasizing the Board's responsibility to collaborate with federal agencies, including NIST, and the private sector. The Board's main tasks include analyzing cyber attacks, gauging technology risks, establishing communication channels for cybersecurity threats, recommending tabletop exercises, and assisting in developing best practices.

Tristan Allen, Cybersecurity and Critical Infrastructure Protection Unit Manager at WMD, is responsible for standing up the new Cybersecurity Advisory Committee, also mandated by 2SSB 5518, to strengthen cybersecurity in both industry and public sectors across all critical infrastructure sectors. He shared their committee will focus on broader cross-sector collaboration in cybersecurity planning, identifying potential representation from sectors like energy, state agencies, healthcare, telecommunications, credit unions, water utilities, and academia. He anticipates a committee size around 20 members. Tristan will attend TSB Security Subcommittee meetings as an observer to ensure alignment between the two committees.

State & Local Government Cybersecurity Grant Program – Zack

Zack Hudgins, WaTech Privacy Manager, gave an overview of the program. The program's planning committee, comprising about 16 members, was established in November 2022 and has met monthly since its inception. In May, they released a notice of intent to gauge the interest of local governments in cybersecurity initiatives. This resulted in over a hundred responses, providing a preview of the projects that would be submitted. By June, the committee had finalized their plan, which was promptly approved by the Federal Emergency Management Agency (FEMA) and Cybersecurity & Infrastructure Security Agency (CISA). The next step involved collecting applications for funding projects. They received applications from 99 entities across the state, totaling over 143 projects.

Zack reviewed the diversity of applications received, emphasizing the program's broad outreach beyond major cities. The submitted projects totaled a request of over $15 million, highlighting the keen interest and pressing need for cybersecurity funding across the state. The planning committee is finalizing the scoring and ranking of the projects to be considered for funding.

Through this program, the committee aims to build capacity and ensure sustainable cybersecurity improvements for entities across the state.

Additional information can be found on the State & Local Cybersecurity Grant Program website.

Security Policy & Standard Review – Bill, Sam, Stevens

Bill reminded members these security policies and standards were developed in a multi-agency, multi-discipline governance structure, where they have been reviewed and recommended for TSB approval.

Bill also reminded members that most of these policy & standard updates are a result of the State Standard 141.10 restructure. Instead of maintaining it as one vast directive, it is being broken out into distinct policies and standards. This way it is easier for state agencies and local government partners to understand and implement and streamlines the process of considering waivers or exceptions.

- **Acceptable Use Policy**: It establishes rules and requirements for the appropriate use of IT assets issued by agencies. It aims to ensure accountability, implementation verification, and additional training for employees to understand and adhere to the policy. A future enhancement to this policy may be a link to a standard that governs the monitoring of endpoints and computing devices.
- **Change Management Policy**: Change management involves effectively managing and controlling changes to an organization's environment, minimizing unknown or risky changes, and implementing processes, training, and policies to ensure successful outcomes by tracking and documenting all changes made.
- **Configuration Management Standard:** The focus is on establishing an easy to implement configuration baseline for technology used by agencies. The goal is to adhere to benchmarks, track configuration baselines, and identify and record deviations to minimize risks introduced into the environment.
- **International Travel Security Policy & Standard**: The new policy and standard addresses the need for technical approval for accessing resources from outside the country during official travels, distinct from financial and business approvals. It was developed in response to a need expressed by Dept. of Ecology. The policy ensures devices traveling internationally meet specific criteria and have appropriate visibility and risk management.
- **Vulnerability Management Standard**: This standard helps agencies prioritize vulnerability and patching activities by severity threshold, as well as helps agencies track vulnerability and patching activities.

Members reviewed the draft policies and standards, and recommended them for final approval at the Sept. 14 full board meeting.

Whole State Approach to Cybersecurity – Ralph

Ralph Johnson, State Chief Information Security Officer, explained the whole state approach to cybersecurity is an integrated method that stresses the importance of collaboration across various tiers of government, educational institutions, tribal entities, and other public and private sector organizations. Its primary goal is to counteract cybersecurity threats by fostering open communication and resource sharing and dismantling governmental silos. This strategy enables entities throughout an entire state to collectively strengthen their security defenses.

Ralph further discussed the implementation of a Strategic Threat Intelligence Center (STIC). This is essentially a Security Operation Center, but more advanced. It would collect and analyze data from participating entities, acting as a centralized hub for cybersecurity intelligence. Its function is not only to monitor and respond to immediate threats but also to share this intelligence across all member organizations. The goal is proactive defense, where threats identified in one area can be communicated to others, making them aware and better prepared. He envisions this center to be run by a governing body made of representatives from all participant entities, ensuring diverse inputs and decentralized control. Initial planning with potential stakeholders has taken place and funding options are being considered.

Public Comment

No public comments.

Public meeting adjourned at 10:30 a.m. so the subcommittee and select staff could convene an executive session to discuss recent cybersecurity threats.