WaTech
Washington Technology Solutions

Technology Services Board (TSB)
Security Subcommittee Meeting Minutes

November 9, 2023
9:00 a.m. – 11:00 a.m.
Member Attendees: Bill Kehoe, David Danner, Cami Feek, Viggo Forde, Tracy Guerin, Tanya Kumar, Sen. Joe Nguyen
Hybrid – 1500 Jefferson St SE, Olympia, WA; Presentation Room and Virtual via Zoom

---

Welcome, Agenda Review, 8/18/23 Minutes Review – Bill

Bill Kehoe, TSB Chair, welcomed everyone to the meeting, announcing that Ralph Johnson, State Chief Information Security Officer, will be Chair of this subcommittee. Bill will remain a Co-Chair. He reviewed the agenda for the day, reviewed the Aug. 18 meeting minutes, which were then approved by the attending members.

Review details and requirements of SB 5518 (RCW 43.105.291) – Ralph

Second Substitute Senate Bill 5518, which formalized the creation of the Technology Services Board (TSB) Security Subcommittee.

Ralph reviewed the implementation of Senate Bill 5518, codified into RCW 43.105.291, which aims to strengthen cybersecurity in Washington State. The bill, supported by earlier legislation, highlights the importance of protecting state infrastructure, including municipal and private sectors. The Security Subcommittee has been tasked with broadening its membership beyond TSB members to include diverse technology sectors. This expansion is part of a larger effort to coordinate cybersecurity efforts across state infrastructure, municipalities, and private sectors. The subcommittee is also responsible for reviewing cyber threats, assessing risks to state agency IT, recommending improvements in reporting systems, assisting in the development of cybersecurity best practices, and contributing to the Annual State Cyber Security Report. This subcommittee will also oversee conducting tabletop exercises and will collaborate with the Military Department's Cyber Security team.

Review of Draft Charter – Ralph

Ralph discussed the initial draft charter for this subcommittee. The charter, to be reviewed in February for modifications based on member recommendations and comments, aims for final approval by the TSB full Board in March. Its core purpose is to enhance the security posture of Washington State, address information security risks with urgency, and safeguard state data and infrastructure. The proposed diverse membership includes 19 individuals from various sectors, aiming for a breadth of experience and knowledge. Meetings will be held quarterly for two hours, in a hybrid format, focusing on security topics, risks, threats, and alignment with state cybersecurity objectives. The charter also mandates an annual review or more

frequently if necessary. Ralph encouraged feedback on the draft and open communication for any clarifications.

Security Policy & Standard Review – Ralph, Sam

Ralph reminded members these security policies and standards are an overhaul of existing information security policy and standards, previously encapsulated in the cumbersome and complex document 141.10. The decision was made to break it down into smaller, more digestible documents. These revisions draw upon 141.10 but are enhanced with industry best practices from the NIST Cybersecurity Framework (CFS) and the Center for Internet Security control set. Additionally, gaps are filled using other resources like the ISO 27000 standards, NIST's 800-53, and their Risk Management Framework, ensuring comprehensive coverage beyond the scope of the NIST CSF alone. This approach aims to make the policy more accessible and practical for users.

The following policies and standards were reviewed:

- **Audit & Accountability Standard**: Requires agencies to conduct independent audits every three years with more clearly defined parameters. These changes aim to standardize audit procedures and independent auditor qualifications, ensuring consistency across audits and enabling comparative analysis within the enterprise.
- **Disaster Recovery Planning Policy**: Requires each agency to develop, publish, and ensure availability of a disaster recovery and business continuity plan, shifting the exercise frequency from annual to biennial for better achievability. This policy was also reviewed by the Military Department's Continuity of Operations (COOP) committee, including disaster recovery experts for their feedback resulting in a more practical and clear understanding of disaster recovery needs across agencies.
- **Information Security & Privacy Awareness Training Policy:** Requires security awareness training for all employees within the first 30 days of employment and annually thereafter. This policy, integrating security and privacy, provides a foundation for a comprehensive training program addressing threats like phishing and malware, with additional plans for a separate privacy policy to address concerns about the overlap of security and privacy roles.
- **Physical & Environmental Protection Policy:** Establishes requirements for the physical and environmental protection of IT systems on-premises, including state data centers and other agency locations. It sets a baseline minimum requirement for controlled areas, acknowledging that specific scenarios like HIPAA, CJIS, and IRS Publication 1075 may necessitate additional measures, which agencies must comply with based on their circumstances.
- **Remote Access Standard:** Requires agencies to use WaTech-approved remote access solutions and restricts access to the State Government Network (SGN) to only authorized state-owned equipment. This standard, resulting from extensive discussions and feedback, allows for flexibility in solutions through the Security Design Review (SDR) process, ensuring secure and controlled access to the SGN.
- **Security Assessment & Authorization Policy**: Centers on the Security Design Review (SDR) process, requiring agencies to conduct IT risk assessments for maintenance and new development of systems and infrastructure projects under certain circumstances, and to include SDR results in the system application authorization process. It ensures compliance with state policies and best practices, and requires a plan for addressing deficiencies and implementing compensating controls.

The development of these policies and standards involved a collaborative process, including input and approval from work groups, the IT Security community, CIOs, and various governance and management councils, with continuous modifications to enhance clarity and usability for agencies.

Attending members recommended all six policies and standards for final approval at the next full board meeting on Nov. 28.

State and Local Government Cybersecurity Grant Program – Bill

Bill reviewed the latest status from the cybersecurity grant program, funded by the Infrastructure Investment and Jobs Act of 2021, which allocated $1 billion over four years for state and local cybersecurity improvements. Washington state received $3.7 million for the first year, with a focus on supporting local governments, especially rural communities, to enhance their cybersecurity infrastructure. The program saw over 143 applications, with 114 projects approved, emphasizing upgrades like switching to .gov domains, closing audit findings, incident response plans, multi-factor authentication, and firewall implementations.

The process involved a detailed application and review system, managed in partnership with the Military Department and other federal agencies like DHS and FEMA. In its second year, the program anticipates distributing even larger funds, aiming to assist more local governments and close additional security gaps. The focus is also on guiding jurisdictions whose projects were not initially funded, offering advice for resubmitting applications in the next cycle. The success of this program highlights a significant stride in improving statewide cybersecurity.

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

Executive Session for Members and Select Staff Only – Closed to the Public

The subcommittee and select staff convened an executive session to discuss recent cybersecurity threats and returned to the public meeting.

Public Comment

No public comments.