WaTech
Washington Technology Solutions

Technology Services Board (TSB)
Security Subcommittee Meeting Minutes

February 8, 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 – Bill Kehoe & Ralph Johnson

Bill Kehoe, TSB Chair, called the meeting to order at 9:00 am. and took roll call. Ralph Johnson, Chair, reviewed the agenda and minutes from the November 9, 2023 meeting.

Overview of SSSB 5518/RCW 43.105.291 – Ralph Johnson

Substitute Senate Bill 5518, now codified into RCW 43.105.291, establishes a subcommittee tasked with strengthening cybersecurity within the state. The subcommittee's activities include reviewing emergency cybersecurity attacks and risks, developing a risk assessment program, and issuing an annual cybersecurity report. Membership includes representatives from the TSB, state agencies, local, tribal, territorial agencies, and industry experts. The subcommittee works jointly with the military departments on critical infrastructure cybersecurity and holds joint meetings to prepare the annual report due on December 1st. The subcommittee also provides advice, recommendations, and policies to enhance cybersecurity across the state. The subcommittee operates under the Emergency Management Council and collaborates with the Critical Infrastructure Advisory Committee to explore cyber postures across critical infrastructure sectors, providing sector-specific or cross-cutting recommendations to the legislature.

Final Charter Review – Ralph Johnson

Ralph reviewed the proposed charter changes with the board, noting sections from another subgroup's charter were added, including details about open public meetings, public comments, meeting minutes, travel for non-government employees, ethics, and media. Ralph sought consensus to accept these changes and move the document forward to the full TSB for approval, clarifying that the voting process is based on consensus rather than a numerical count. Members expressed no concerns about the edits and agreed to move the charter forward.

Subcommittee Membership Discussion – Ralph Johnson

Ralph reviewed the current status of the subcommittee members and noted that there are still vacant slots for additional local government, industry, and agency representatives. Recommendations for suitable candidates are welcome. The goal is to finalize the membership by

the end of March, prioritizing individuals who will actively participate and engage in the committee's work.

Overview of the Office of Cybersecurity – Ralph Johnson

Ralph presented on the Office of Cybersecurity (OCS) within WaTech, providing insight into its functions and structure. The OCS was officially codified in legislation three years ago, with a mission to promote and facilitate effective information security. The vision is to establish Washington State OCS as a national leader in protecting information assets.

The OCS comprises four branches: Policy and Program, Information Security Services, Security Operations, and Security Engineering. The Policy and Program branch focuses on statewide policies, risk assessments, and outreach. The Information Security Services branch serves as the security team for WaTech and 17 small agencies, ensuring compliance and supporting audits. The Security Engineering branch conducts security design reviews and addresses architectural issues. Lastly, the Security Operations branch manages the security operations center, the CERT team, and threat hunting, providing operational security platforms and vulnerability management statewide.

Enterprise Security Service Highlight: Vulnerability Management – Ralph Johnson

Ralph discussed the importance of vulnerability management as a key function of a security operations center. He highlighted that managing vulnerabilities reduces the potential impact of threats, but it cannot eliminate risk entirely. The presentation covered the vulnerability management life cycle, including identifying vulnerabilities through scanning systems, evaluating them for severity and impact, treating them by applying patches or making configuration changes, and reporting the findings to relevant stakeholders. He emphasized the need for agencies to act promptly on vulnerability reports and to prioritize remediation efforts based on the severity and potential impact of vulnerabilities. He also mentioned the importance of standardizing asset management practices as a prerequisite for effective vulnerability management.

Policy & Standard Review – Ralph Johnson and Sam Zee

Ralph reviewed the following policies with the board:

1. **Mobile Device Usage Policy**: Updates include sections on data retention policies, issuance of mobile devices, and utilization guidelines for both state-issued and personally-owned devices.

2. **Mobile Device Security Standard**: Focuses on state-issued devices, requiring encryption for category three and four data, application of mobile device management (MDM) software, maintaining current operating systems, and preventing auto-launching of non-agency approved applications.

3. **Non-Agency Issued Device Security Standard**: Similar to the state-issued standard but with additional requirements, such as a written agreement for personal device use, MDM software, and prevention of auto-launching non-agency approved applications.

4. **Application Security Standard**: Ensures that data processed in applications is not disclosed, altered, or destroyed without authorization. Requires a risk assessment for application vulnerabilities prior to production.

5. **Encryption Standard**: Requires encryption for data in motion and at rest, with a change to remove the FIPS mode requirement unless mandated by federal or other regulations.

6. **Security Logging Standard**: Requires agencies to configure security logging to specified standards to detect, identify, and respond to security events and policy violations.

7. **Privacy and Data Protection Policy**: A new enterprise policy separating privacy requirements from security roles. Highlights include formalizing privacy impact assessments and requiring agencies to have a designated privacy contact.

Ralph sought agreement to advance the policies for adoption by the Technology Services Board, and all present concurred.

10:35 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 10:55 am; no action was taken.

Public Comment

No public comments were received.

The meeting was adjourned at 11:00 am.

TSB Security Subcommittee Members Present: Ralph Johnson, *Chair*, Bill Kehoe, *Co-chair*, David Danner, Tracy Guerin, Cammy Feek, Andreas Bohman, Vigo Forde

Submitted by Leanne Woods, Board & Committee Program Administrator