WaTech
Washington Technology Solutions

Technology Services Board

Security Subcommittee Meeting
November 9, 2023
9:00 am – 11:00 am

WaTech
Washington Technology Solutions

Current TSB Members

Industry Members
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 (Security Subcomm.)

WaTech
Washington Technology Solutions

Agenda

TOPIC	LEAD	PURPOSE	TIME
Welcome | Agenda review	Bill Kehoe	Introductory remarks	9:00 a.m.
Review and approve August 10 meeting minutes	Bill Kehoe	**Approval** of minutes	9:10 a.m.
Review details and requirements of SB 5518 (RCW 43.105.291)	Ralph Johnson	Discussion	9:15 a.m.
Review of Draft Charter	Ralph Johnson	Discussion	9:30 a.m.
Policies & Standards review: • Audit & Accountability Standard • Disaster Recovery Planning Policy • Information Security & Privacy Awareness Training Policy • Physical & Environmental Protection Policy • Remote Access Standard • Security Assessment & Authorization Policy	Ralph Johnson Sam Zee	**Review and Recommend Approval** to full Board on 11/28	9:50 a.m.
State & Local Government Cybersecurity Grant Program	Bill Kehoe	Status/Board discussion	10:10 a.m.
Transition to Executive Session			10:25 a.m.
Executive Session for members and select staff only – Closed to public	Ralph Johnson		10:30 a.m.
Transition from Executive Session back to Public Meeting			10:50 a.m.
Public comment			10:55 a.m.

WaTech
Washington Technology Solutions

Review 8/10/23 Minutes

WaTech
Washington Technology Solutions

Review details and requirements of SB 5518 (RCW 43.105.291)

WaTech
Washington Technology Solutions

Technology Services Board Security Subcommittee

Purpose: Provide advice, recommendations, and policies 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 for providing 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.

Activities:

- Review emergent cyberattacks and threats to critical infrastructure sectors to identify 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, treatment opportunities, and projected shortfalls.
- Recommend tabletop cybersecurity exercises, including data breach simulation exercises.
- Assist the Office of Cybersecurity in developing best practice recommendations for state agencies.
- Review proposed policies and standards developed by the Office of Cybersecurity and recommend their approval to the full board.
- Review information relating to cybersecurity and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies.
- Assist in developing the annual state of cybersecurity report.

WaTech
Washington Technology Solutions

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 related 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

Review of Draft Charter

Technology Services Board
Security Subcommittee

Purpose:

To work together with a shared dedication to enhancing the security posture of Washington state as outlined in RCW 43.105.291. Address information security risks with urgency and regularly assess tools and services in the State of Washington ecosystem to achieve the objectives and safeguard the data and infrastructure of Washington state.

Objectives:

As defined in RCW 43.105.291, the subcommittee will work to achieve ……

Membership:

- State Chief Information Security Officer – Chair
- Technology Services Board Chair (State Chief Information Officer) – Co-Chair
- Chair of the Military Department's Cybersecurity Advisory Committee
- (3) Technology Service Board Members
- (1) WaTech Executive Team Representative
- (1) Military Department Representative (in addition to the Chair of the Cybersecurity Advisory Committee
- (2) Deputies from the Office of Cybersecurity
- (3) Local Government Representatives
- (3) Industry Representatives
- (2) Agency CIO/CISO Representatives
- (1) Representative from the Attorney General's Office

Meetings:

Meetings will be held quarterly and scheduled for two hours unless otherwise designated.

The subcommittee will hold at least one joint meeting annually with the Military Department's Cybersecurity Advisory Committee.

Each meeting will discuss important security topics and events occurring in the state.

Attendance at quarterly meetings will be in person and remote.

Charter Review:

At least annually.

WaTech
Washington Technology Solutions

Security Policy and Standard Review

WaTech
Washington Technology Solutions

Audit and Accountability Standard

Purpose of Action

- Request approval standard and rescind 141.10 section 1.6.

Business Case

- Audits help agencies identify areas of non-compliance.
- Agencies require a risk-based mechanism to request a time-bound compliance waiver.

Key Objectives

- Specify requirements agencies must follow when performing **independent** IT Audits.
- Require agencies to determine the cause of non-conformities to **inform a risk-based control strategy**.
- Require agencies to **document** an audit nonconformity **resolution plan**.

Strategic Alignment

- This policy supports both achieving compliance with state security policies/ standards and the risk-based management of compliance nonconformities.

Implementation

- Agencies must ensure the independence of the team performing an audit, whether internal or external.
- Agencies must coordinate with the State Auditor's Office to ensure audits align with agreed-upon audit procedures.
- Agencies must develop a root-cause analysis process to analyze audit findings.

Success Criteria

- **Measurable:** Agency IT audit performance procedures will ensure consistent IT audits.
- **Timebound:** Agencies will perform audits every three years as required.
- **Equitable:** Agencies of all sizes benefit from independent IT audits. Consistent auditing standards ensure agencies have clear expectations.

WaTech
Washington Technology Solutions

Disaster Recovery Policy

Purpose of Action

Request policy approval and rescind Policy 151.

Business Case

- Disaster recovery planning ensures mission critical, and business essential functions continue to operate as smoothly as possible during and after any kind of crisis.
- Contingency plans can be created in advance to restore interrupted business operations..

Key Objectives

- Create a **common understanding** of disaster recovery planning requirements.
- Require **exercising** of disaster recovery plans to validate recovery and contingency procedures.

Strategic Alignment

Disaster recovery planning strengthens IT architecture security. Documentation of planning and validation supports accountable government.

Implementation

- Templates will help agencies develop disaster recovery plans.
- Training and time for testing from key staff is needed.
- Training and exercising plans will require coordinated efforts for interdependent systems

Success Criteria

- **Achievable:** Small agencies may contract WaTech for support. All agencies can rely on WaTech for templates and advice.
- **Relevant**: The lessons learned from COVID can inform new DR plans.
- **Equitable:** Each agency determines what is critical or essential to their mission and creates a plan unique to their needs.

WaTech
Washington Technology Solutions

Information Security & Privacy Awareness Training Policy

Purpose of action

- Request approval of policy and rescinding of old policy version.

Business case

- Ensures agency staff have awareness and training aligned with their role in IT security.
- Requires basic cybersecurity awareness training for all IT system users because everyone has a role in preventing a breach.

Key Objectives

- Ensure that users are familiar with potential threats to the IT ecosystem and aware of strategies they must employ to prevent or respond to those threats.
- Agency staff who have IT and IT security-related roles are informed and recognize their roles and responsibilities.

Strategic alignment

- Supports efficient and accountable government by ensuring agencies are managing IT roles and responsibilities comprehensively.

Implementation

- Agencies will need review and verify that their awareness and training requirements are sufficient
- Agencies may request additional training and support.
- Additional specific training cannot be designated where not in a job description, but training paths can be suggested.

Success criteria

- Activity and feedback on the awareness and training materials can be reported.
- Agency IT system users attest to their awareness of their duties and obligations.

WaTech
Washington Technology Solutions

Physical & Environmental Protection Policy

Purpose of Action

This standard expands on 141.10 (3) requirements, establishing information technology physical and environmental protect controls.

Business Case

Agencies controlling physical spaces housing information technology which stores and/or processes state data must secure those areas against environmental or physical threats.

Key Objectives

Specify the requirements for effective physical and environmental controls.

Strategic Alignment

This policy supports efficient and accountable government by ensuring agencies are managing IT resources comprehensively.

Implementation

Agencies must align its internal physical and environmental procedures to align with this policy.

Success Criteria

- Agencies will provide evidence of their physical and environmental (P&E) controls.
- Agencies will providence evidence that their P&E controls align with their mission risks.
- Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

WaTech
Washington Technology Solutions

Remote Access Standard

Purpose of Action

This standard updates 141.10 (6.4) by requiring the use of WaTech-approved remote access solutions. It also specifies that only agency-owned or approved devices can use the common remote access services.

Business Case

This standard ensures accountability and the implementation of controls for remote access to the State Government Network.

Key Objectives

Ensure that users employ WaTech-approved remote access methods.

Strategic Alignment

This policy supports proactive cyber solutions and practices by requiring the use of approved common remote access services.

Implementation

Agencies will configure their remote access solution in accordance with this standard.

Success Criteria

- Agencies will use WaTech approved remote access methods.
- Analysis of the remote connection logs collected by the Office of Cybersecurity and host agencies will evidence compliance.
- Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

WaTech
Washington Technology Solutions

Security Assessment and Authorization Policy

Purpose of Action

- Request policy approval and rescind sections 1.2.1 and 1.5 of 141.10 Securing IT Assets Standard.

Business Case

- The system authorization process considers the risks of operating that system and the controls applied to mitigate those risks.
- The Security Design Review ensures document of a system's compliance with State security standard is documented prior to deployment.

Key Objectives

- Identify risks and available mitigations to protect state data and make informed business decisions.
- Describe when a security design review is required and agency responsibilities for security design reviews.

Strategic Alignment

- This policy supports efficient and accountable government by ensuring agencies are managing IT roles and responsibilities comprehensively. .

Implementation

- Agencies must complete an IT risk assessment of the proposed IT system or application upon receipt of the SDR results.
- Agencies must include the SDR results in its systems/application authorization process.

Success Criteria

- **Measurable:** SDR records will reflect appropriate applications/systems receive Security Design Reviews prior to authorization.
- **Achievable:** Agencies will provide evidence of a completed IT risk assessment for all systems/applications new systems/applications authorized by the agency to operate.

WaTech
Washington Technology Solutions

State & Local Government Cybersecurity Grant Program Update

Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program (SLCGP), appropriating $1 billion to be awarded over four years (FY 22 – 25).

DHS has implemented the SLCGP through CISA and the Federal Emergency Management Agency (FEMA).

- CISA will serve as the program management subject-matter expert in cybersecurity related issues.
- FEMA will provide grant administration and oversight for appropriated funds, including award and allocation of funds to eligible entities, financial management, and oversight of funds execution.

States and territories will use their State Administrative Agencies (SAAs) to receive SLCGP funds from the federal government and then distribute the funding to local governments in accordance with state law and procedures

DHS issued the SLCGP Notice of Funding Opportunity (NOFO) in August 2023. The NOFO includes all requirements and details, including information on funding eligibility for states and territories.

The established SAA for states and territories will be the only entities that can apply for grant awards under the SLCGP, with local entities receiving sub-awards through states.

Eligible entities can apply via Grants.gov.

- Applications may include a completed Cybersecurity Plan, capabilities assessment, and individual projects approved by the Cybersecurity Planning Committee and CIO/CISO/equivalent.
- Entities without a completed plan are encouraged to apply and submit it by September 30, 2023. This requirement must be completed and submitted in year one, to be eligible for year two funding.

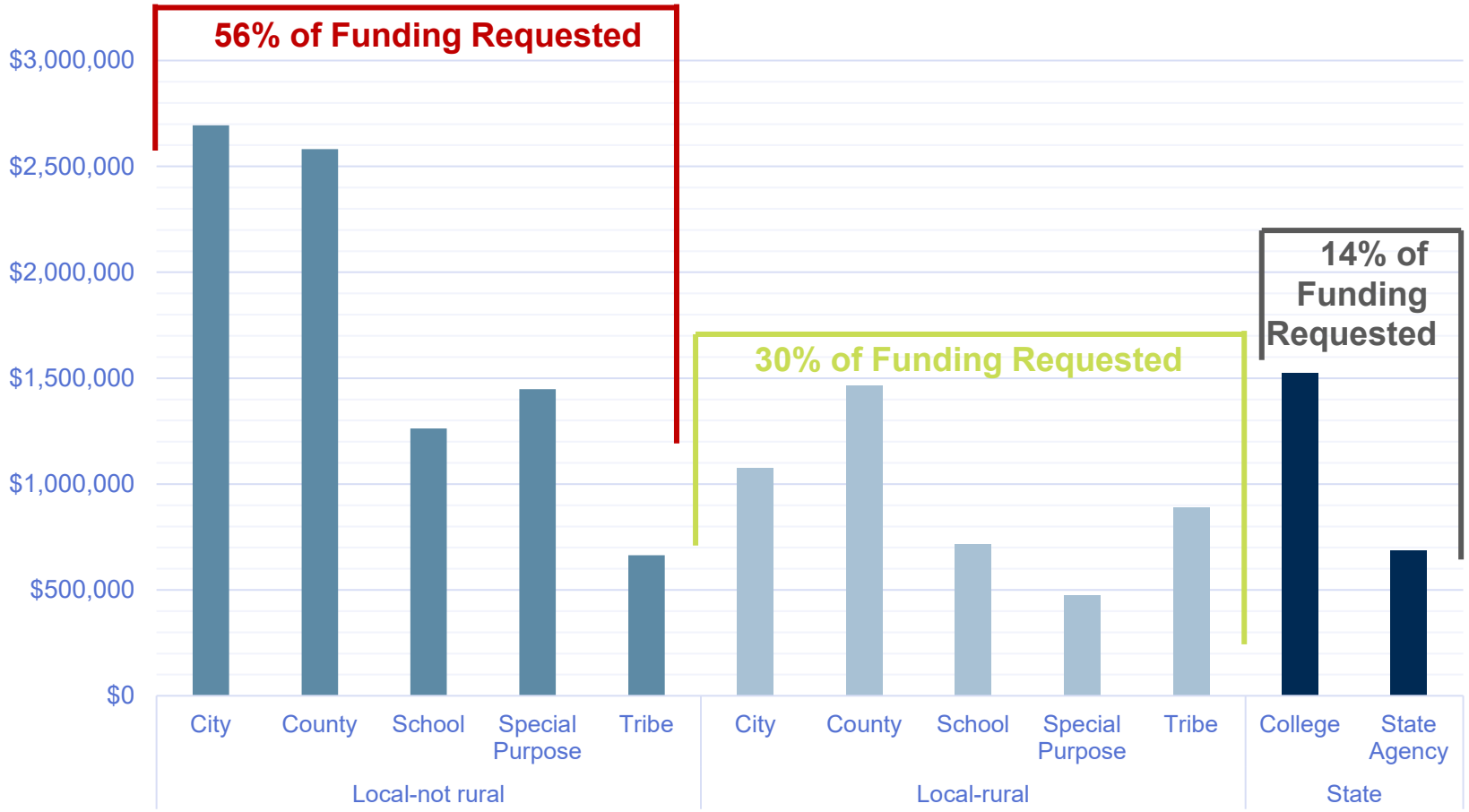
Cybersecurity Planning Committee formed and meeting since November 2022.

Statewide Cybersecurity Plan sent and approved by CISA, June 2023.

Local Government Application Review Process

- The Planning Committee reviewed, scored, ranked, and recommended projects for funding.
- Projects approved by State CIO - August 2023.

Total Requested by Funding Type

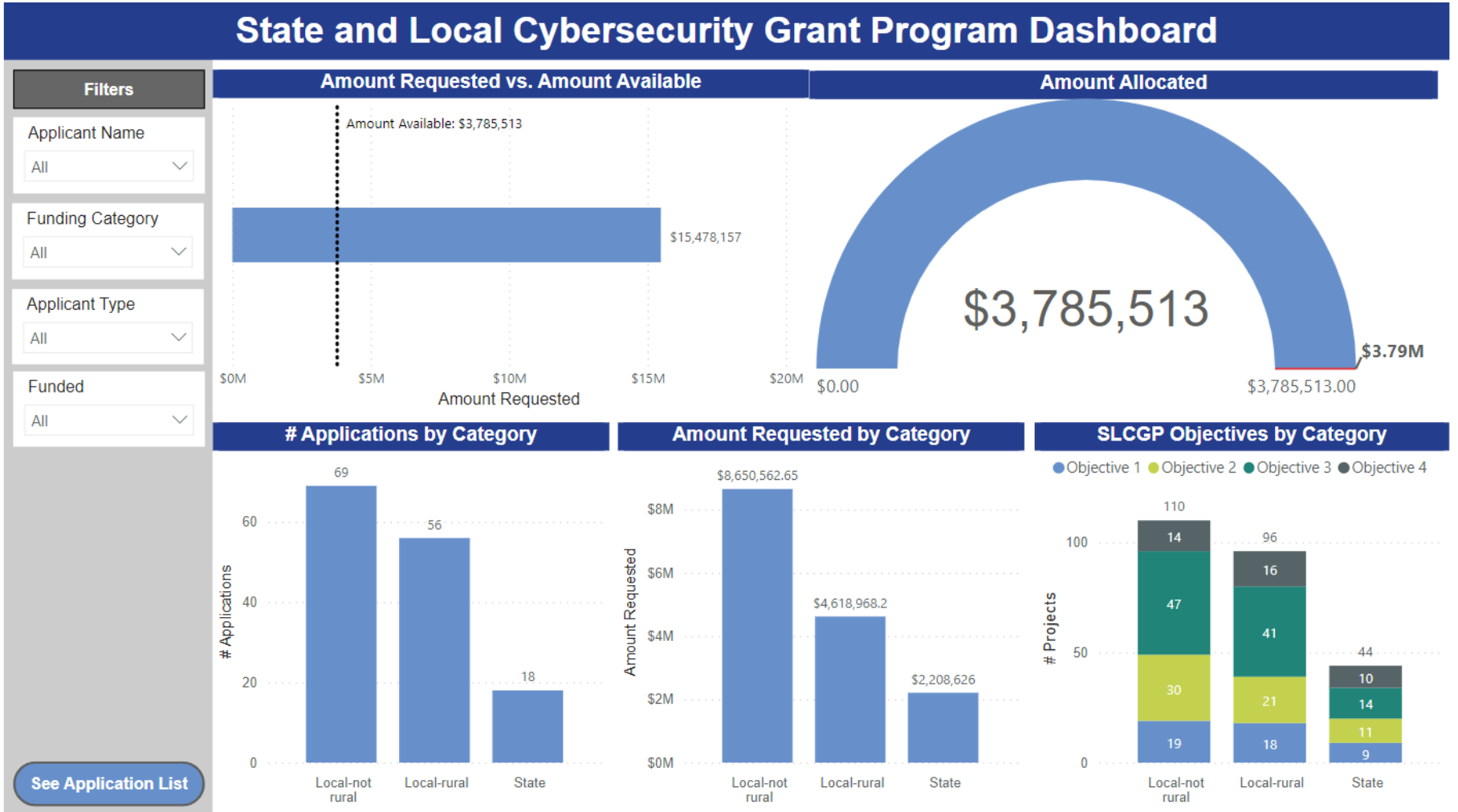


Projects

Themes

- Cybersecurity program assessment and development
- Domain change to .gov
- Response to SAO audits.
- Critical infrastructure (SCADA) security controls
- Incident response and recovery plan and tabletop exercises
- Penetration testing and vulnerability assessment services
- Firewalls and security platforms and services
- Identity management and MFA
- Diversity of Training needs from platform and product-specific, security awareness to professional training and certifications.

- [SLCGP Dashboard - Power BI (powerbigov.us)]



FY22 Funding Update (provided by MIL 11/7)

All projects approved by CISA!

Funding released by FEMA

- Agreements will be sent to sub-recipients before 12/10
- Subrecipients start projects
  - Reimbursement and Reporting workbooks emailed end of November
  - Nationwide Cybersecurity Review (NCSR) needs to be completed by **12/1/2023**
  - Reporting due in January

FY23 status update:

- FY22 project request debriefs continue; Resubmittals coming back in for review.
- FY23 state application for year two sent to CISA/FEMA
- FY23 process update
  - Lessons learned in the process (November 2 meeting)
- FY23 New application round target open Spring 2024

WaTech
Washington Technology Solutions

Transition to Executive Session

Executive Session in progress.

Resuming public meeting at 10:55 a.m.

Public comment