WaTech
Washington Technology Solutions

Technology Services Board

Security Subcommittee Meeting
February 8, 2024
9:00 am – 11:00 am

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.)

Agenda

TOPIC	LEAD	PURPOSE	TIME
Welcome | Agenda review | 11/9 Minutes review	Ralph Johnson	Introductory remarks	9:00 a.m.
Overview of SSSB 5518 / RCW 43.105.291	Ralph Johnson Tristan Allen	Information	9:10 a.m.
Final Charter Review	Ralph Johnson	Review and Recommendation	9:15 a.m.
Subcommittee Membership Discussion	Ralph Johnson	Member Discussion	9:30 a.m.
Overview of the Office of Cybersecurity	Ralph Johnson	Information	9:40 a.m.
Enterprise Security Service Highlight: Vulnerability Management	Ralph Johnson	Information	9:55 a.m.
Policies & Standards review: • Agency Mobile Device Usage Policy ○ Mobile Device Security Standard ○ Non-Agency Issued Device Security Standard • Application Security Standard • Encryption Standard • Security Logging Standard • Privacy and Data Protection Policy	Ralph Johnson Katy Ruckle Sam Zee	**Review and Recommend Approval** to full Board on 03/12/24	10:15 a.m.
Executive Session RCW 43.105.291(4): Members & Select Staff Only	Ralph Johnson	Discuss Sensitive Security Topics and Information	10:35 a.m.
Public comment			10:55 a.m.
Adjournment			11:00 a.m.

WaTech
Washington Technology Solutions

Review 11/9/23 Minutes

WaTech
Washington Technology Solutions

Overview of SSSB 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.

SSB 5518
Creation of the Technology Services Board Security Subcommittee

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.

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.

WaTech
Washington Technology Solutions

Final Charter Review

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.

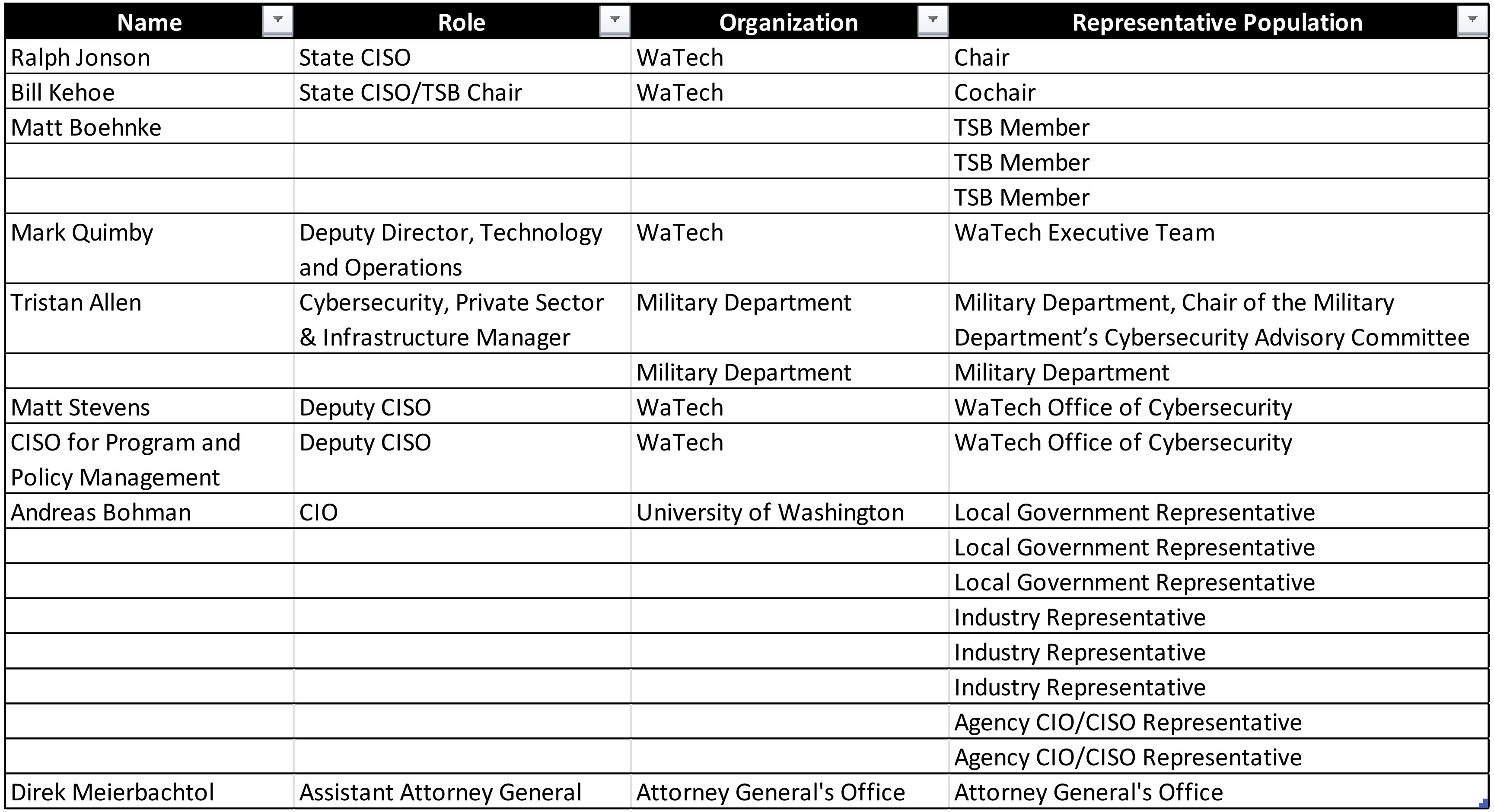
Charter Review:

At least annually.

WaTech
Washington Technology Solutions

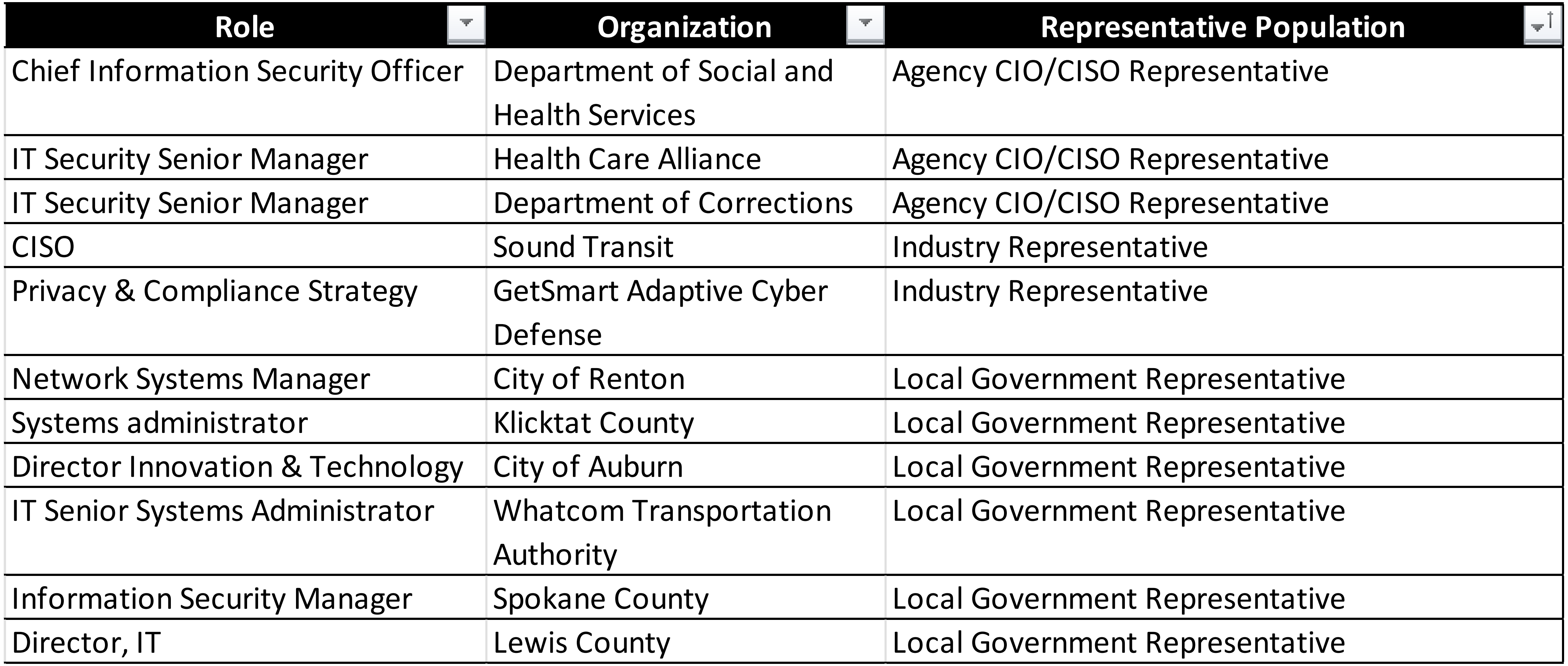
Subcommittee Membership Discussion

Confirmed Membership



Name	Role	Organization	Representative Population
Ralph Jonson	State CISO	WaTech	Chair
Bill Kehoe	State CISO/TSB Chair	WaTech	Cochair
Matt Boehnke			TSB Member
			TSB Member
			TSB Member
Mark Quimby	Deputy Director, Technology and Operations	WaTech	WaTech Executive Team
Tristan Allen	Cybersecurity, Private Sector & Infrastructure Manager	Military Department	Military Department, Chair of the Military Department’s Cybersecurity Advisory Committee
		Military Department	Military Department
Matt Stevens	Deputy CISO	WaTech	WaTech Office of Cybersecurity
CISO for Program and Policy Management	Deputy CISO	WaTech	WaTech Office of Cybersecurity
Andreas Bohman	CIO	University of Washington	Local Government Representative
			Local Government Representative
			Local Government Representative
			Industry Representative
			Industry Representative
			Industry Representative
			Agency CIO/CISO Representative
			Agency CIO/CISO Representative
Direk Meierbachtol	Assistant Attorney General	Attorney General's Office	Attorney General's Office

Potential Members (volunteered)



Role	Organization	Representative Population
Chief Information Security Officer	Department of Social and Health Services	Agency CIO/CISO Representative
IT Security Senior Manager	Health Care Alliance	Agency CIO/CISO Representative
IT Security Senior Manager	Department of Corrections	Agency CIO/CISO Representative
CISO	Sound Transit	Industry Representative
Privacy & Compliance Strategy	GetSmart Adaptive Cyber Defense	Industry Representative
Network Systems Manager	City of Renton	Local Government Representative
Systems administrator	Klicktat County	Local Government Representative
Director Innovation & Technology	City of Auburn	Local Government Representative
IT Senior Systems Administrator	Whatcom Transportation Authority	Local Government Representative
Information Security Manager	Spokane County	Local Government Representative
Director, IT	Lewis County	Local Government Representative

WaTech
Washington Technology Solutions

Overview of the Office of Cybersecurity

RCW 43.105.450 Office of cybersecurity

The office of cybersecurity is created within the office of the chief information officer (WaTech).

The director shall appoint a state chief information security officer, who is the director of the office of cybersecurity.

Mission & Vision

Vision:

Establish Washington State OCS as a model and national leader in the protection of information assets.

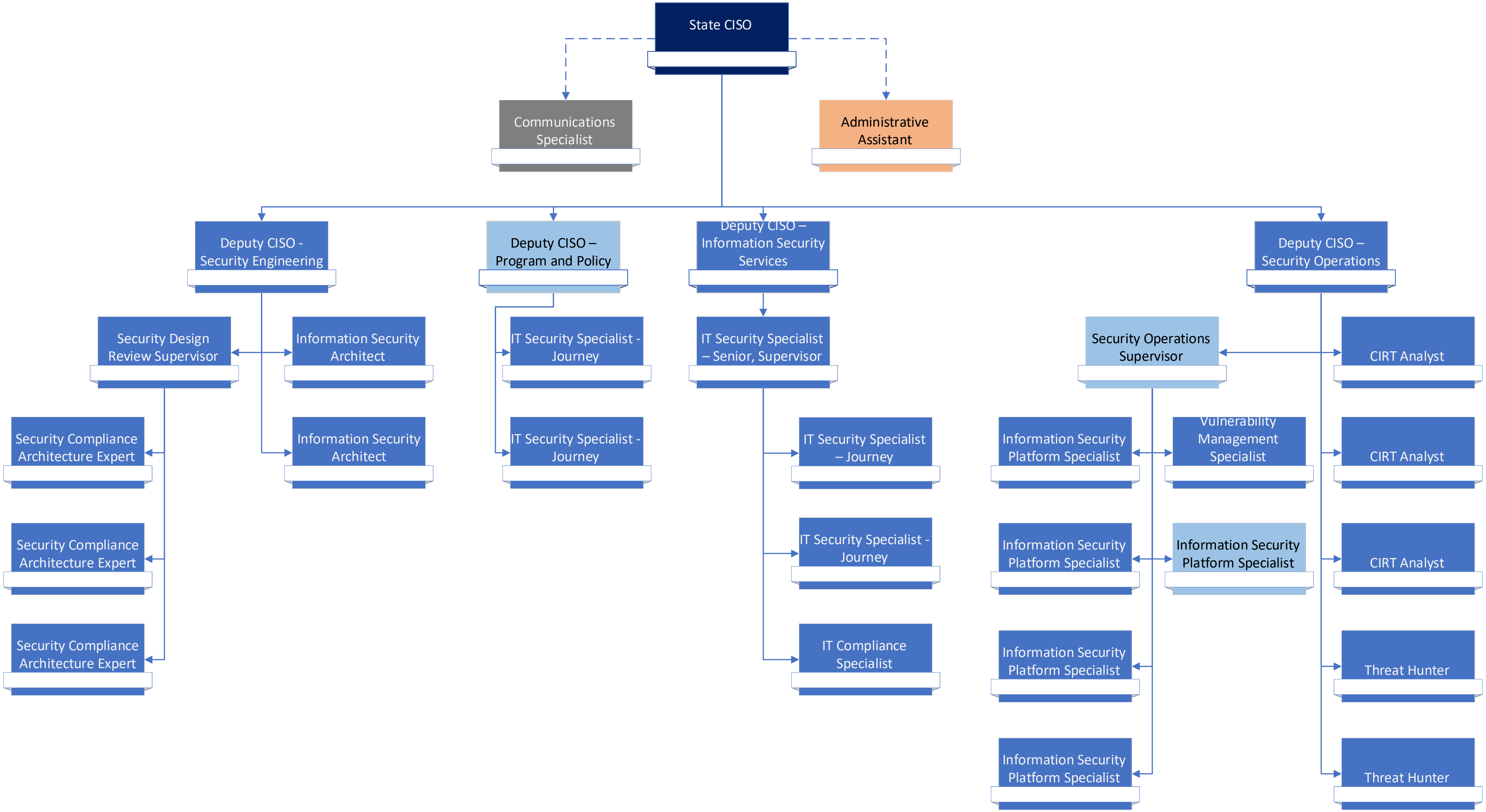
Mission:

Promote and facilitate effective information security.

Value Proposition:

Ensure a high degree of information security in the daily activities of Washington State agencies, commissions, workforce members, and partners (private and public) while supporting their business operations.

Office of Cybersecurity (OCS)



State CISO

Communications Specialist

Administrative Assistant

Deputy CISO - Security Engineering

Security Design Review Supervisor

Security Compliance Architecture Expert

Security Compliance Architecture Expert

Security Compliance Architecture Expert

Information Security Architect

Information Security Architect

Deputy CISO – Program and Policy

IT Security Specialist - Journey

IT Security Specialist - Journey

Deputy CISO – Information Security Services

IT Security Specialist – Senior, Supervisor

IT Security Specialist – Journey

IT Security Specialist - Journey

IT Compliance Specialist

Deputy CISO – Security Operations

Security Operations Supervisor

Information Security Platform Specialist

Vulnerability Management Specialist

Information Security Platform Specialist

Information Security Platform Specialist

Information Security Platform Specialist

Information Security Platform Specialist

CIRT Analyst

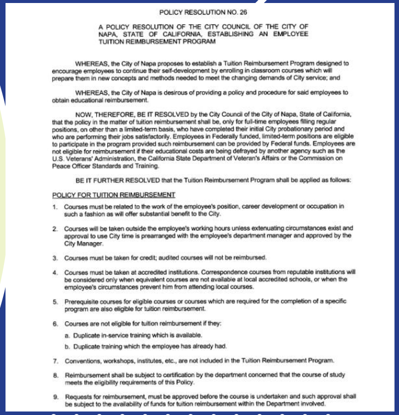
CIRT Analyst

CIRT Analyst

Threat Hunter

Threat Hunter

Program and Policy Management



POLICY RESOLUTION NO. 26

A POLICY RESOLUTION OF THE CITY COUNCIL OF THE CITY OF NAPA, STATE OF CALIFORNIA, ESTABLISHING AN EMPLOYEE TUITION REIMBURSEMENT PROGRAM

WHEREAS, the City of Napa proposes to establish a Tuition Reimbursement Program designed to encourage employees to continue their self-development by enrolling in classroom courses which will prepare them in new concepts and methods needed to meet the changing demands of City service; and

WHEREAS, the City of Napa is desirous of providing a policy and procedure for said employees to obtain educational reimbursement.

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Napa, State of California, that the policy in the matter of tuition reimbursement shall be, only for full-time employees filling regular positions, on other than a limited-term basis, who have completed their initial City probationary period and who are performing their jobs satisfactorily. Employees in Federally funded, limited-term positions are eligible to participate in the program provided such reimbursement can be provided by Federal funds. Employees are not eligible for reimbursement if their educational costs are being defrayed by another agency such as the U.S. Veterans' Administration, the California State Department of Veteran's Affairs or the Commission on Peace Officer Standards and Training.

BE IT FURTHER RESOLVED that the Tuition Reimbursement Program shall be applied as follows:

POLICY FOR TUITION REIMBURSEMENT

1. Courses must be related to the work of the employee's position, career development or occupation in such a fashion as will offer substantial benefit to the City.
2. Courses will be taken outside the employee's working hours unless extenuating circumstances exist and approval to use City time is prearranged with the employee's department manager and approved by the City Manager.
3. Courses must be taken for credit; audited courses will not be reimbursed.
4. Courses must be taken at accredited institutions. Correspondence courses from reputable institutions will be considered only when equivalent courses are not available at local accredited schools, or when the employee's circumstances prevent him from attending local courses.
5. Prerequisite courses for eligible courses or courses which are required for the completion of a specific program are also eligible for tuition reimbursement.
6. Courses are not eligible for tuition reimbursement if they:
   a. Duplicate in-service training which is available.
   b. Duplicate training which the employee has already had.
7. Conventions, workshops, institutes, etc., are not included in the Tuition Reimbursement Program.
8. Reimbursement shall be subject to certification by the department concerned that the course of study meets the eligibility requirements of this Policy.
9. Requests for reimbursement, must be approved before the course is undertaken and such approval shall be subject to the availability of funds for tuition reimbursement within the Department involved.

Focus - Statewide

Statewide Information Security Policy and Standards Management and Maintenance

Statewide Information Security Program Development

Statewide Risk Management

Outreach to Local Jurisdictions

Security Engineering

Focus - Statewide

Information Security Engineering for WaTech Technology Systems

Guidance for Agency Technical System Engineering

Security Design Review Process

WaTech
Washington Technology Solutions

Information Security Services

Focus - WaTech and Small Agency

Serves as CISO and security team for WaTech and 17 Small Agencies

Ensures Security Operations for WaTech and 17 Small Agencies

Assists WaTech and Agencies with compliance audit response

Security Operations

Focus - Statewide

Management of Security Operations Center, Security Incidents, Forensics Analysis

Outreach to Local Jurisdictions for Assistance with Incident Response and Management

WaTech
Washington Technology Solutions

Enterprise Security Service Highlight: Vulnerability Management

Managing VULNERABILITIES reduces the potential that a THREAT can cause an IMPACT.

Reducing RISK.

Risk = Threats x Vulnerabilities x Impact

Vulnerabilities

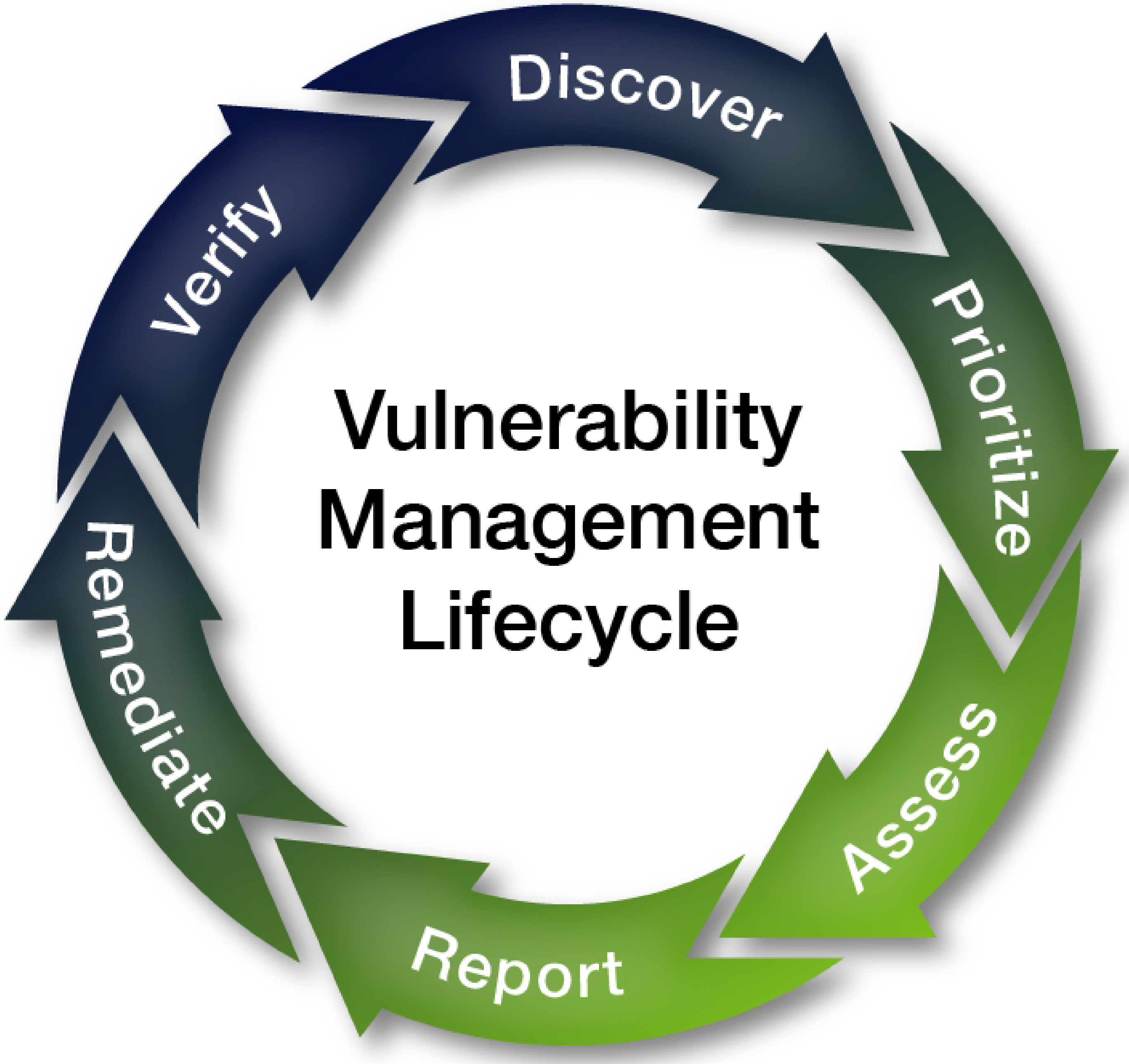
Weaknesses present in a system or process.

Impacts

The effect a threat exploiting a vulnerability will have on the organization.

Threat

Any situation or circumstance with the **potential** to negatively impact the operations of an organization (including mission, functions, image, or reputation), its assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service via an information system.



Vulnerability Management

The process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.

Identifying Vulnerabilities

- Vulnerability Scanning Platform

  A software application designed to assess computers, networks, or applications for known weaknesses. These tools test systems for the presence of vulnerabilities, such as flaws in software, incorrect system configurations, or security loopholes, and provide information on the findings.

- Endpoint Detection and Response Systems

  a category of security solutions that focus on detecting, investigating, and responding to threats at the endpoint level — which includes workstations, servers, and mobile devices.

- External Attack Surface Management Platform

  Helps identify, manage, and protect against potential vulnerabilities of publicly exposed information technology assets and systems.

Evaluating Vulnerabilities

- Vulnerability Analysis:
  - False Positive Elimination.
  - Contextual Analysis.
- Risk Assessment:
  - Severity Rating.
  - Likelihood Determination.
  - Impact Analysis.
- Prioritization:
  - Based on the combination of severity, likelihood of exploitation, and potential impact.
  - Consideration of External Factors

Treating Vulnerabilities

- Remediation Planning:

  Creating a plan to address each vulnerability.

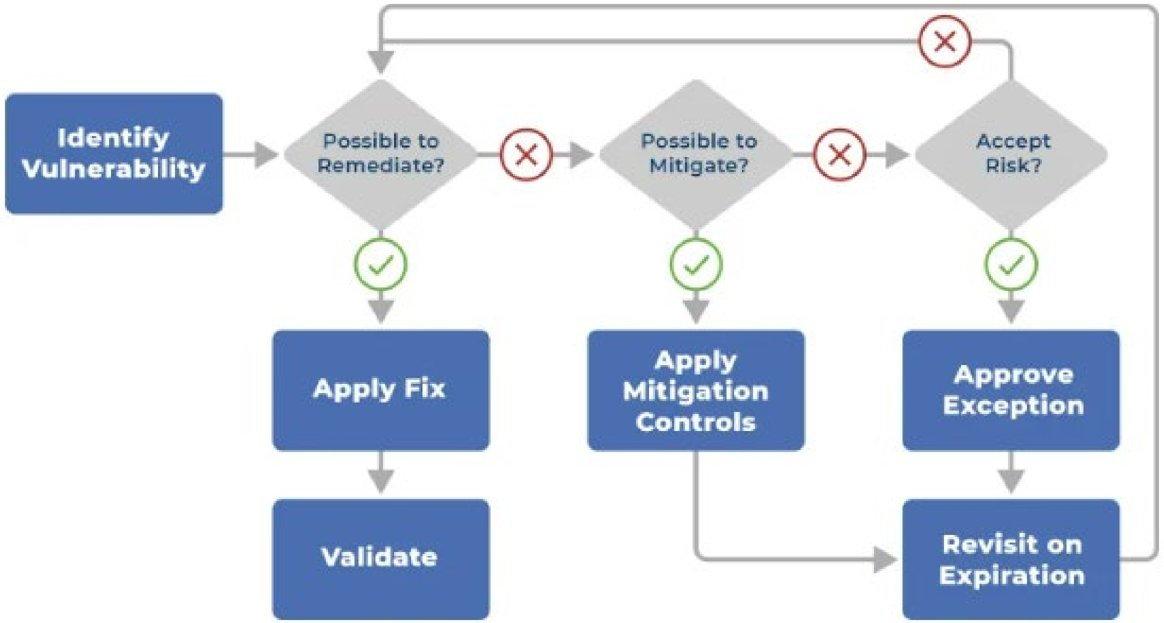
  Resource Allocation.
- Remediation Implementation:

  Applying Patches and Updates.

  Configuration Changes.

  Mitigation Controls.
- Verification:

  Ensuring that the remediation measures are effective.



Securin

Reporting Vulnerabilities

- Vulnerability Management as a Service (VMaaS)

  Monthly agency meetings

- OCS – Agency Consultations

  Vulnerability Management Specialist

```
abort("The Rails environment [illegible]
require 'spec_helper'
require 'rspec/rails'

 require 'capybara/rspec'
 require 'capybara/rails'

 Capybara.javascript_driver = [illegible]
 Category.delete_all; Category[illegible]
 Shoulda::Matchers.configure do |config|
   config.integrate do |with|
     with.test_framework :rspec
     with.library :rails
   end
 end

 # Add additional requires below this line. [illegible]

 # Requires supporting ruby files with [illegible]
 # spec/support/ and its subdirectories. [illegible]
 # run as spec files by default. This means [illegible]
 # in _spec.rb will both be required and [illegible]
 # run twice. It is recommended that you [illegible]
 # end with _spec.rb. You can configure [illegible]
```

WaTech
Washington Technology Solutions

Policy and Standard Review

Agency Mobile Device Usage Policy

- Replaces Mobile Device Usage Policy 191.
- USER policy developed with a security lens.
- Focusses on state-issued devices.
- **NEW requirement** to communicate the agency Mobile Device Usage Policy and procedures when onboarding, annually, and when revised.

Mobile Device Security Standard

- Replaces IT Security Standard 141.10 (5.8).
- Focusses on state-issued devices.
- Requires encryption of data over category 3.
- Requires MDM or EMM software and current mobile OS.
- **NEW requirement** to prevent auto-launching of non-agency approved applications at device start-up.

Non-Agency Issued Device Security Standard

- **NEW Document.**
- Requires written agreement for personal device use.
- Requires MDM or EMM software and current mobile OS.
- **NEW requirement** to prevent auto-launching of non-agency approved applications at device start-up.

Standards for Consideration:

- **Application Security Standard**

  Requires a risk assessment to *identify and plan to resolve application vulnerabilities* prior to production.

- **Encryption Standard**

  Update to require FIPS mode *only when required* by federal partners.

- **Security Logging Standard**

  Establishes minimum requirements for system security log generation to *reconstruct events for business recovery*.

Privacy and Data Protection Policy

- **NEW Document.**
- Enterprise Security Governance requested this policy.
- Outlines existing requirements for Privacy Threshold Analysis (PTA) and Privacy Impact Analysis (PIA) & other existing legal requirements.
- Requires a privacy contact at each agency.

Executive Session in progress.

Resuming public meeting at 10:55 a.m.

Public comment