State Auditor's Office Cybersecurity Update Fiscal Year 2025

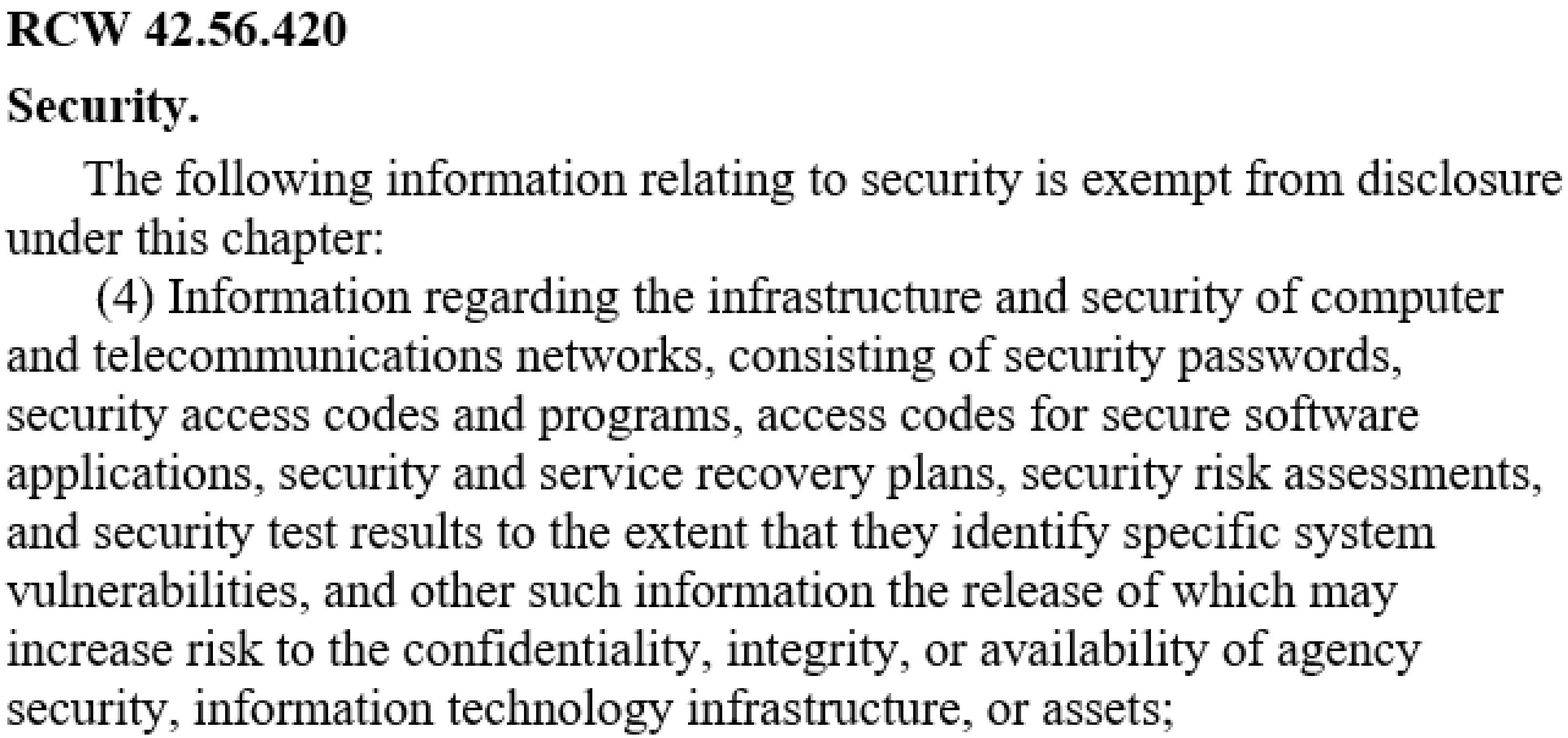
For reports published September 8, 2025

Agenda for today’s presentation

- State Auditor’s Office portfolio of cybersecurity audits
- Continuing Opportunities to Improve State Agency IT Security Organizations – FY 2025
- Continuing Opportunities to Improve Local Government and Critical Infrastructure IT Security – FY 2025
- Additional cybersecurity-related services

Protecting sensitive information

Confidentiality is key



RCW 42.56.420

Security.

The following information relating to security is exempt from disclosure under this chapter:

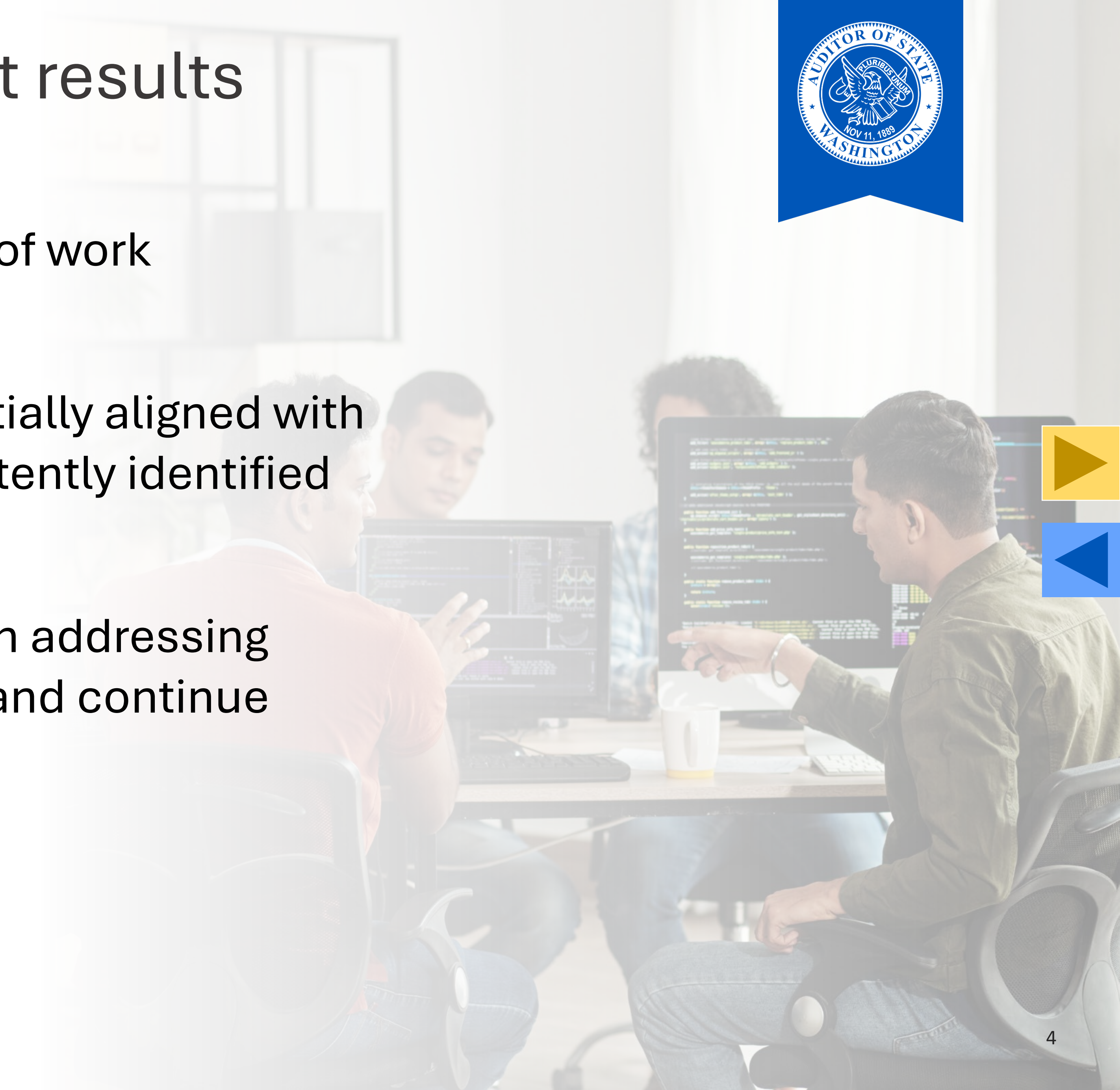
(4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of agency security, information technology infrastructure, or assets;

Delivery of detailed audit results

- Communicated detailed results of work as we completed it

- While policies and practices partially aligned with the selected controls, we consistently identified areas to improve

- Governments have already begun addressing significant issues we identified, and continue to make improvements



Continuing to expand our audit reach

Type of audit	Who is served	Total completed	Year started	In this report period
Cybersecurity	State agencies	46	2013	7
Cybersecurity	Local governments	61	2013	7
Critical infrastructure	Local governments	83	2022	39
Ransomware resiliency	Local governments	9	2023	6

Cybersecurity performance audits underway at:

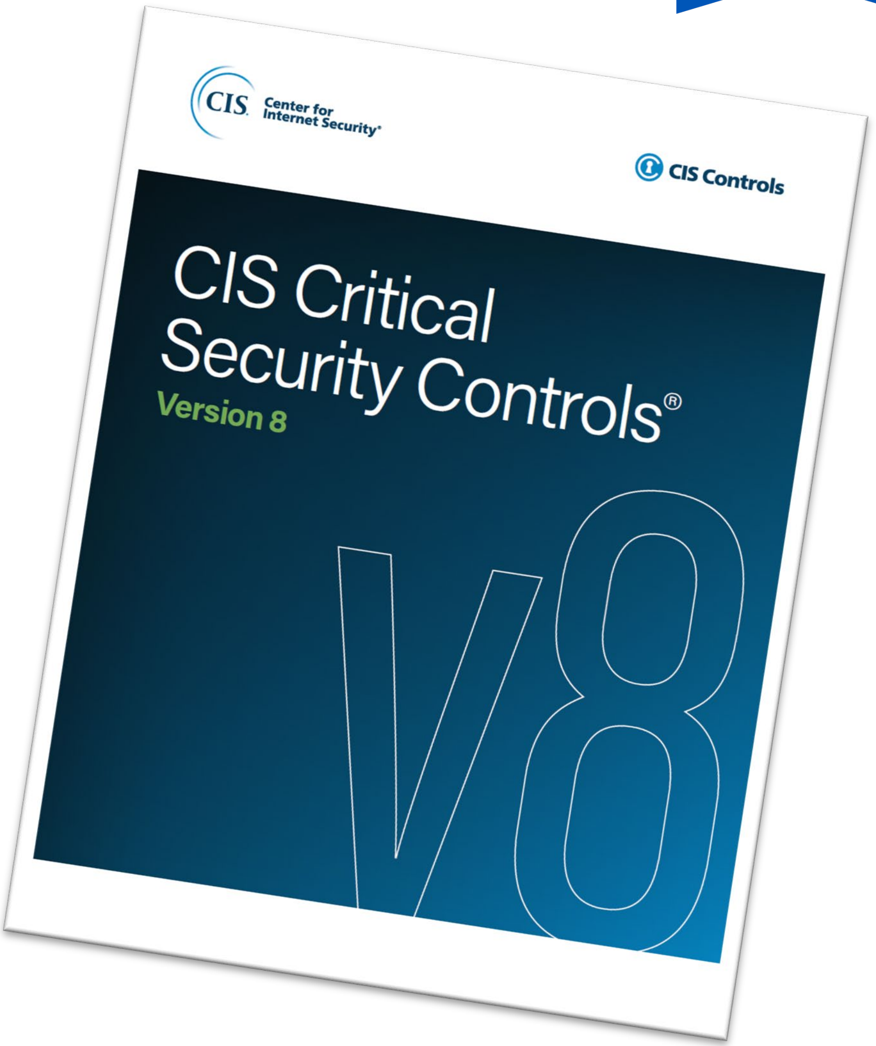
- Six state agencies, 12 local governments, one critical infrastructure local government

Opportunities to Improve IT Security at State Agencies – FY 2025

Audit work completed at seven state agencies

Audits focused on two areas:

- Compared agency practices to selected safeguards from the Center for Internet Security, version 8
- Performed penetration testing of internal network, external network, and selected applications using a vendor



CIS Center for Internet Security®

CIS Controls

CIS Critical Security Controls®

Version 8

v8

State cybersecurity **safeguard** results

- Scope based on size, maturity and specific concerns or efforts of each agency
- Assessed an average of 31 safeguards at each government, out of 153 possible safeguards

61%

Implementation				
All systems	**Most systems**	**Some systems**	**Partially**	**Not in place**
70	34	27	65	20
32%	16%	13%	30%	9%

State cybersecurity **penetration test** results

- Across these seven state agencies, penetration testing was conducted on applications and various network segments

- Identified 227 vulnerabilities of the following severity levels:

Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
3	**21**	46	92	65	227

- The **24** most severe vulnerabilities could more readily be exploited by hackers to cause a security breach

Opportunities to Improve IT Security at Local Governments – FY 2025

Audit work completed at 52 total local governments

- 7 cybersecurity audits
- 6 ransomware resiliency audits
- 39 critical infrastructure audits

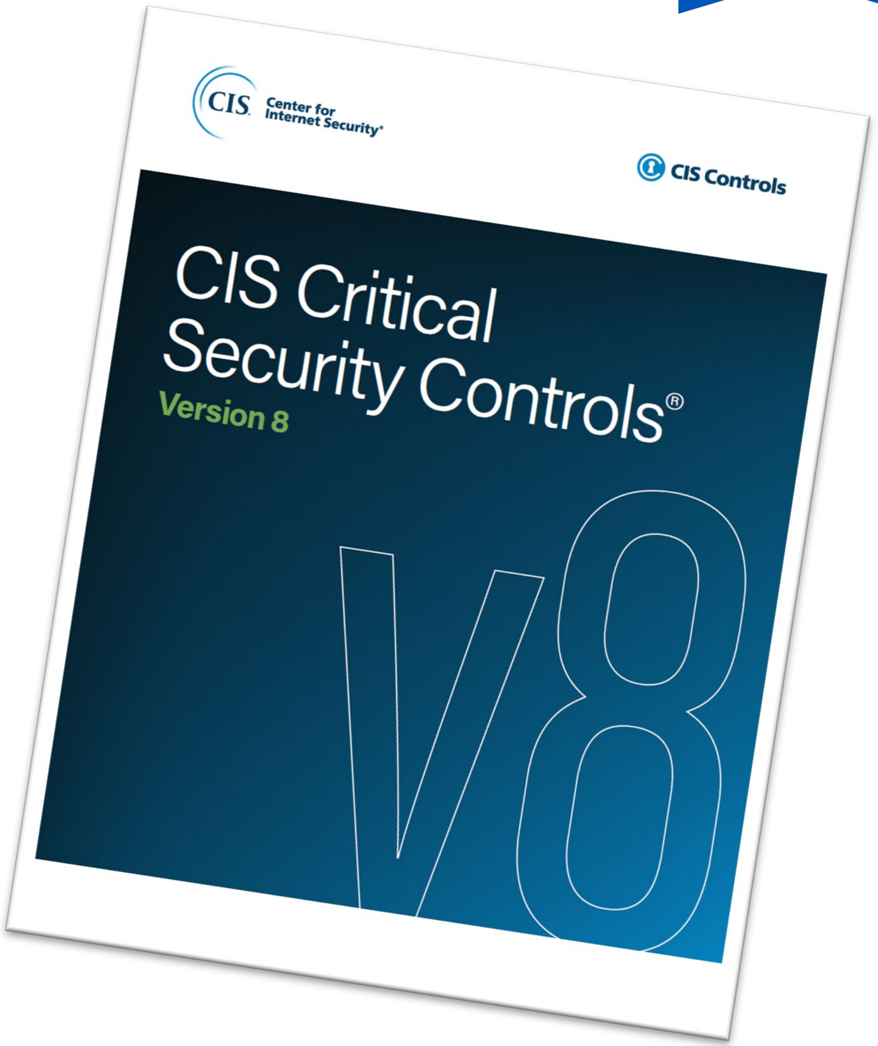
Local cybersecurity audits

- Completed during the fiscal year at seven local governments

- Included assessments work in two areas:

  ✓ Compared local government practices to selected safeguards from the Center for Internet Security, version 8

  ✓ Performed penetration testing of internal network, external network and selected applications using a vendor



CIS Center for Internet Security®

CIS Controls

CIS Critical Security Controls®

Version 8

v8

Local cybersecurity **safeguard** results

- Scope based on size, maturity and specific concerns or efforts of each government
- Assessed an average of 31 safeguards at each government, out of 153 possible safeguards

51%

Implementation				
All systems	**Most systems**	**Some systems**	**Partially**	**Not in place**
49	40	22	76	32
22%	18%	10%	35%	15%

Local cybersecurity **penetration test** results

- Across these seven local governments, penetration testing was conducted on applications and various network segments
- Identified nearly 300 vulnerabilities of the following severity levels:

Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
9	**47**	47	125	55	283

- The **56** most severe vulnerabilities could more readily be exploited by hackers to cause a security breach

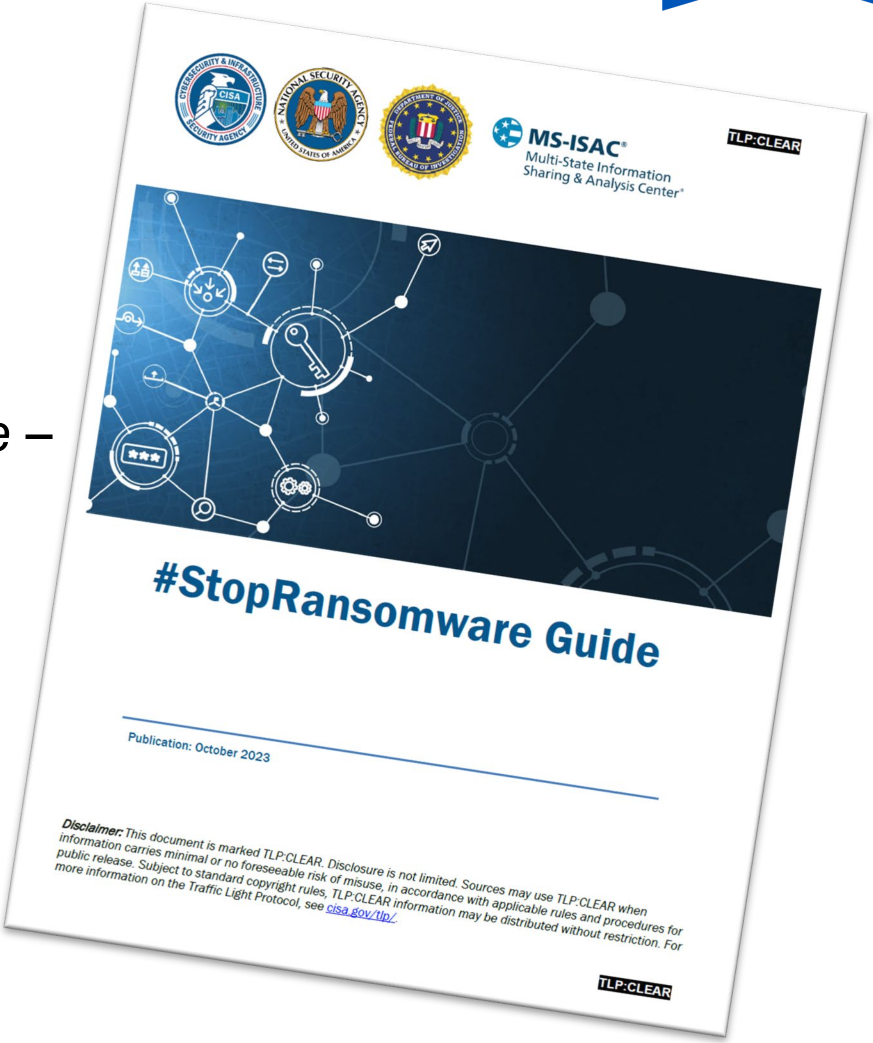
Improving ransomware resiliency and critical infrastructure

Audit work completed in FY 2025 at **local governments** included:

- 6 ransomware resiliency audits
- 39 critical infrastructure audits

Ransomware resiliency audits

- Completed during the fiscal year at six local governments
- Included assessment work in two areas:
  - ✓ Compared local government practices to recommendations from *#StopRansomware* – Joint Ransomware Task Force
  - ✓ Performed vulnerability and technical analysis tied to assessed best practices using Auditor's Office staff and tools



MS-ISAC®
Multi-State Information Sharing & Analysis Center®

TLP:CLEAR

#StopRansomware Guide

Publication: October 2023

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

TLP:CLEAR

Ransomware resiliency audit results

- Assessed the same 22 safeguards at each government
- Focused on technical safeguards that specifically address ransomware detection, response and recovery capabilities
- Due to the technical nature of the safeguards, they were assessed as: fully, partially or not implemented

63%

Implementation		
Fully in place	**Partially**	**Not in place**
32	52	48
24%	39%	36%

Critical infrastructure audits

Focused on local governments providing critical infrastructure, such as water, wastewater, and healthcare

- In response to continuing threat identified by federal authorities
- Primarily an external penetration test to identify external facing vulnerabilities
- Short interviews to compare practices to recommendations from the Cybersecurity & Infrastructure Security Agency

Critical infrastructure audit results

- Audited 39 local governments with critical infrastructure
- Includes high-level review of IT practices
- Primary focus on external penetration testing
- Identified 264 vulnerabilities, with the following severity levels:

Severity					
Critical	High	Medium	Low	Informational & observations	**Total**
1	26	33	128	76	264

Local audit work led to improvements by national vendor

Audit research and penetration testing in Washington in FY 2025 produced a national effect

- Vendor supported many local and national water agencies
- Our testing demonstrated a risk, leading vendor to make significant improvements in IT security for all customers

Statement later issued by federal agencies stressed the same issue, advising the same improvement

Common themes at audited governments

Best results:

- Governments undergoing a repeat audit
- Those with dedicated IT security staff

Good IT security results elsewhere were inconsistent, not always related to IT staffing methods, which also varied:

- No IT staff
- Part-time IT staff
- Vendor-only IT support
- Small IT department without IT security staff

Other cybersecurity-related services from the State Auditor’s Office

#BeCyberSmart Program

The Center for Government Innovation's cybersecurity program offers:

- ➢ Resources
- ➢ Training
- ➢ Presentations
- ➢ Technical advice
- ➢ Cyber checkups

Additional resources, audits and coordination from our Office

- ***It starts with policy – a guide to jump-starting your cybersecurity program:*** Helps local governments create effective IT policies and jump-start their cybersecurity program

- Security attestation engagements (WaTech and Department of Licensing)

- Cyber loss follow-up

CYBERSECURITY
is everyone's job.

Leadership and Planning

Leading the way

Cybersecurity considerations for local government leadership

Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

Information Technology

At the core of cybersecurity

IT staff can help build, integrate and maintain a cybersecurity program

Here are three things you can do in your role to #BeCyberSmart.

Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

Leadership and Planning

It starts with policy

A guide to jump-starting your cybersecurity program

The Office of the Washington State Auditor launched the Cyber Checkup program in 2023, nd one of the common results we have found that local governments lack or need to rove their information technology (IT) umentation, including standards, dures and most importantly, policies.

re what different groups om your IT policies to erSmart.

Office of the Washington State Auditor
Pat McCarthy

September 2024

Contact information

Pat McCarthy

State Auditor

Pat.McCarthy@sao.wa.gov

(564) 999-0950

Scott Frank

Director of Performance & IT Audit

Scott.Frank@sao.wa.gov

(564) 999-0809

Quinn Peralta

IT Security Assistant Audit Manager

Quinn.Peralta@sao.wa.gov

(564) 201-2953

Website: www.sao.wa.gov
X: @WAStateAuditor
Facebook: www.facebook.com/WaStateAuditorsOffice
LinkedIn: Washington State Auditor’s Office