Office of the Washington State Auditor
Pat McCarthy

State Auditor's Office 2022 Cybersecurity Report

Published February 2, 2023

What's in this year's roundup report?

- Continued importance of cybersecurity
- Continuing Opportunities to Improve State IT Security – 2022
- Opportunities to Improve Information Technology Security at Critical Infrastructure Organizations – 2022
- Additional cybersecurity efforts at the State Auditor's Office

Continued importance of cybersecurity

In 2021, ransomware affected more than 2,300 local governments, schools and healthcare providers across the country.

Russia's invasion of Ukraine increased concerns around targeted attacks on U.S. critical infrastructure

- **January 2022:**
  America's Cybersecurity & Infrastructure Security Agency (CISA), the FBI and the National Security Agency (NSA) issued an alert urging heightened security awareness at critical infrastructure companies, including government agencies.

About the State Auditor's Office cybersecurity audits

We conduct cybersecurity performance audits at

- State agencies
- Local governments

Work typically includes:

- Penetration testing
- Assessing IT security controls against leading practices

New for 2022: Critical infrastructure audits that included:

- External network penetration testing
- Open-Source Intelligence (OSINT)

We continue to expand our audit reach

Currently auditing two state agencies, nine local governments and 16 critical infrastructure organizations

Year	State agencies	Local governments	CI entities
2014-15	6	0	
2016	3	1	
2017	3	1	
2018	3	4	
2019	4	7	
2020	5	8	
2021	6	9	
2022	4	8	20
Total	**34** (includes 3 repeats)	**38**	**20**

Data in the table includes audits published as of 12/31/2022.

Continuing Opportunities to Improve State IT Security – 2022

State agency cybersecurity audit conducted in 2022

This performance audit included:

- Two large agencies, one medium agency, one small agency
- Eighth in this series of audits, covering 31 unique agencies
- Assessed network and application security and IT security practices

Protecting sensitive information under Washington state law

Confidentiality is key, and state law limits what we can report publicly. It includes specific details of testing that can put government systems at risk.

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;

Audit question: Can selected agencies make their IT systems more secure?

- Penetration testing of four agencies' network and applications
  - ✓ External
  - ✓ Internal
- Performed by contracted subject matter experts

State and local cybersecurity audits – penetration testing results

Across 62 audits since 2017, we have conducted penetration testing on almost 400 applications and hundreds of network segments.

- We identified more than 2,600 vulnerabilities of the following severity levels:

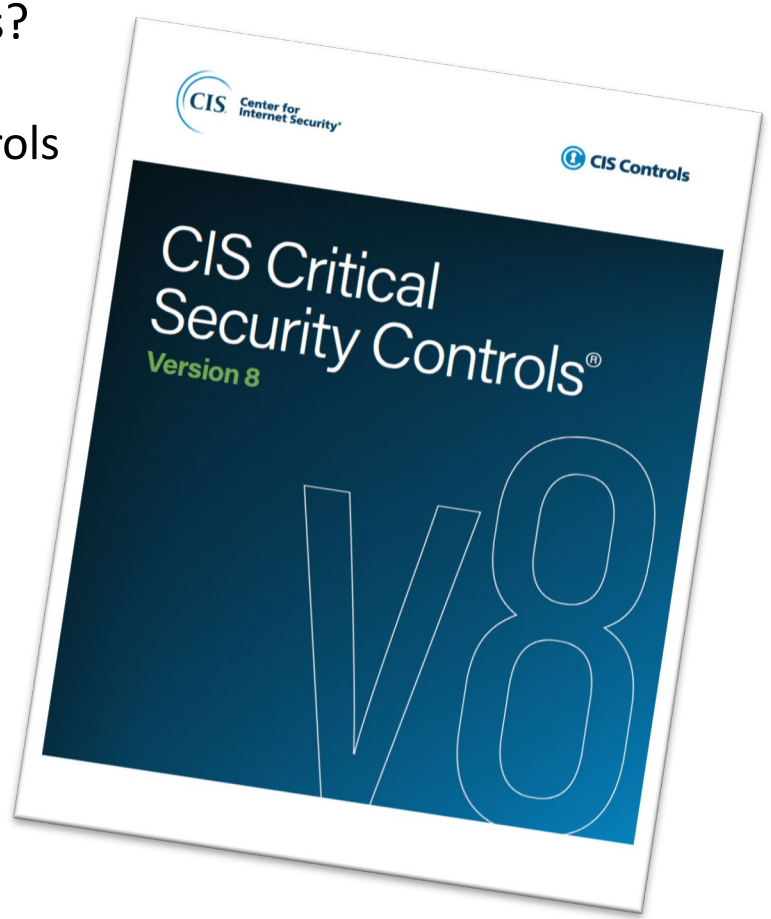
Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
64	**608**	451	1040	518	2,681

- The **672** most severe vulnerabilities could be exploited by hackers to cause a security breach.

Second question concerned IT security practices compared to leading practices

Can state agencies better align their IT security practices with leading practices?

- We compared agency practices to controls from the Center for Internet Security. These controls are:
  - ✓ Informed by private- and public-sector stakeholders
  - ✓ Prioritize benefits
- Our audit program applied material from versions 7.1 and 8 of the CIS Controls.



The CIS Controls we considered

The audit evaluated agency practices against CIS Controls, including:

- Inventory and control of hardware assets
- Inventory and control of software assets
- Data protection
- Secure configurations for hardware and software
- Account management
- Continuous vulnerability management
- Controlled use of administrative privileges
- Audit log management
- Data recovery
- Incident response management
- Secure configuration for network devices

Audit results help generate change

We communicated detailed results of work to each agency as we completed it.

- While agencies' policies and practices partially aligned with the CIS Controls, we identified areas to improve.
- Agencies have already begun addressing significant issues we identified, and continue to make improvements.

Improving IT Security at Critical Infrastructure Organizations

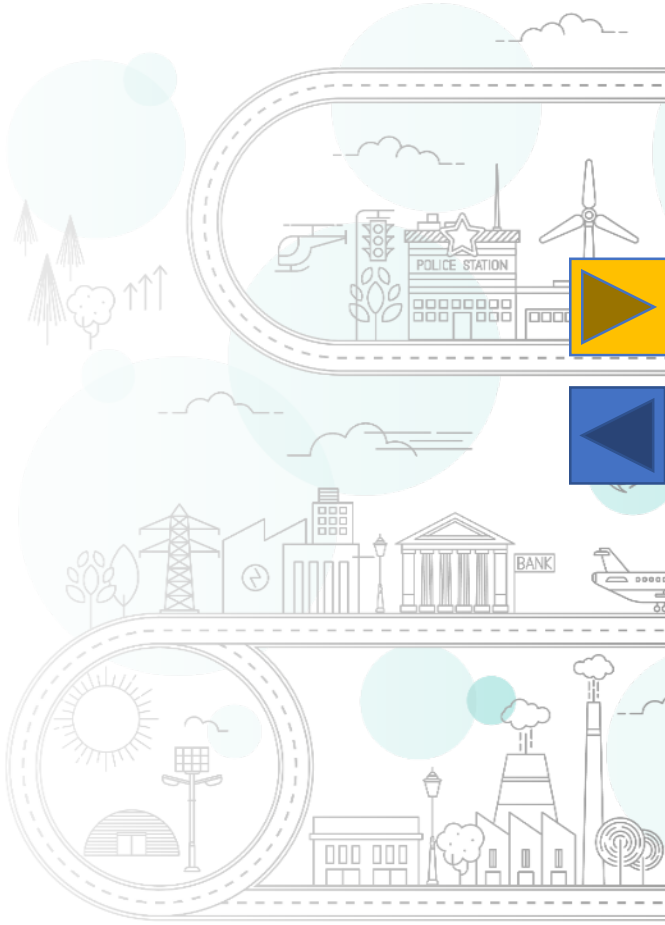
Why audit cybersecurity at critical infrastructure organizations?

We saw the January 2022 joint cybersecurity advisory as a call to action. Our Office was well positioned to examine IT security in this area.

Work focused on local governments providing critical infrastructure, such as:

- Hospitals
- Energy
- Water
- Sewer

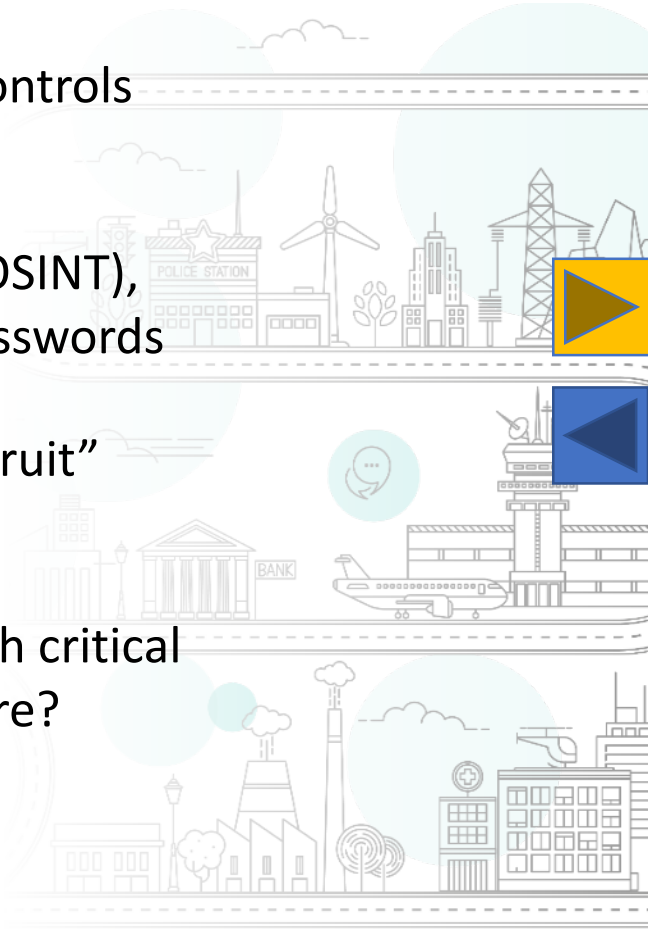
- Auditees selected with input from state stakeholders, to make greatest impact using our existing audit resources.



How we approached our work

- Interviews to identify areas for improvement
- Penetration testing of internet-facing industrial controls systems and other assets
- Open-source intelligence assessment (known as OSINT), considering information such as compromised passwords
- Smaller scope intended to identify “low-hanging fruit”

Audit question: Can selected local governments with critical infrastructure improve their external security posture?



Efficient use of audit resources producing useful results

- Narrower scope meant:
  - Less staff time needed at local government and for our auditors
  - More audits completed more quickly
- Audited 20 local governments with critical infrastructure, with 16 more under way
- We issue tailored recommendations for critical systems according to risks and needs

Critical Infrastructure audit results

OSINT discovered breaches which included:

- Compromised passwords for non-government accounts using government email addresses
- Exposed employee information
- Potential indicators of compromise

External penetration testing identified 122 vulnerabilities, with the following severity levels:

Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
0	**22**	25	31	44	122

Audited governments have already begun addressing significant issues.

Additional cybersecurity efforts at the State Auditor's Office

Security attestation engagements

What is required by Washington's Office of Chief Information Officer (OCIO):

- Triennial attestation engagement
- Compliance with OCIO security standards
- We build the audit program
- Conduct the audits under contracts with agencies

- We have a similar arrangement with the Department of Licensing.

Cyber Loss follow-up work

A “cyber loss” is a social engineering attack where:

- Someone poses as a vendor or employee
- Convinces the government to divert payroll, vendor payments or gift cards to them instead of correct account

Since 2016, state agencies and local governments have reported 111 cyber losses totaling more than $25 million.

Through follow-up work, our auditors:

- Determine the cause
- Evaluate actions taken to prevent reoccurrence
- Make recommendations for additional measures

Security topics now incorporated into many routine accountability audits

Accountability audits determine whether governments have controls in place to protect public resources.

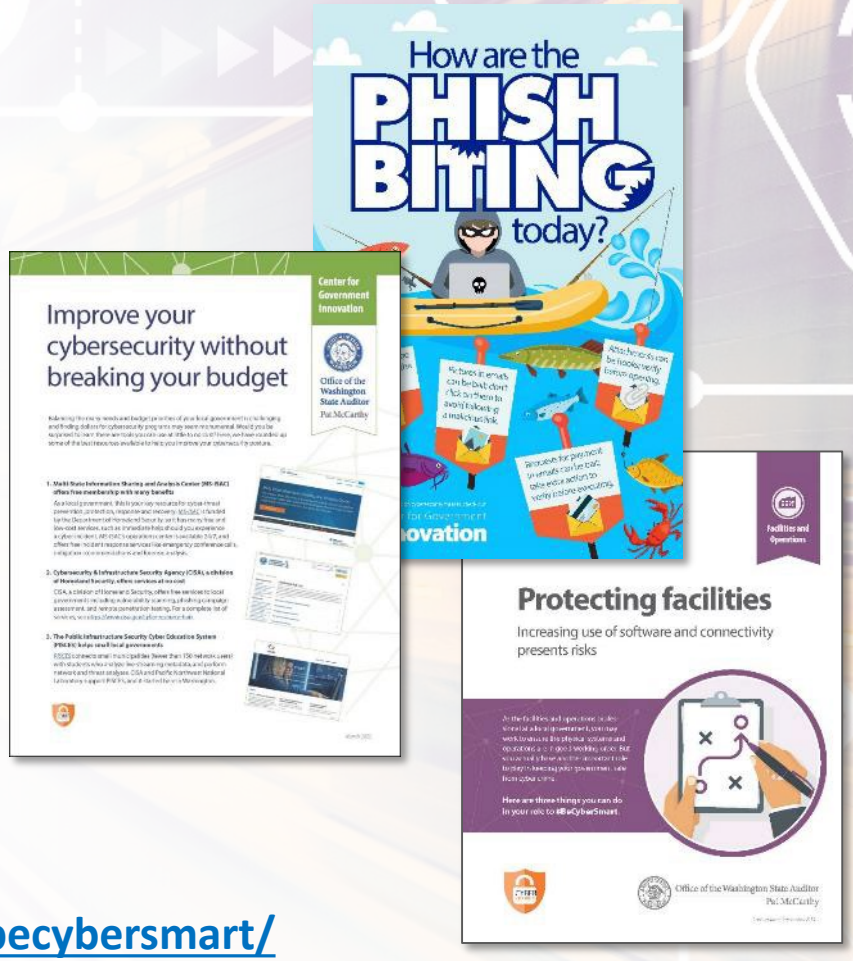
- Auditors can incorporate several topics into these audits:
  - ✓ Backup and recovery
  - ✓ User access
  - ✓ Patch management
- Programs include: Testing strategy, auditor training, technical assistance from our IT auditors and security specialists

These efforts extend our cybersecurity work to hundreds of additional local governments.

#BeCyberSmart Program

The Center for Government Innovation's cybersecurity program offers:

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

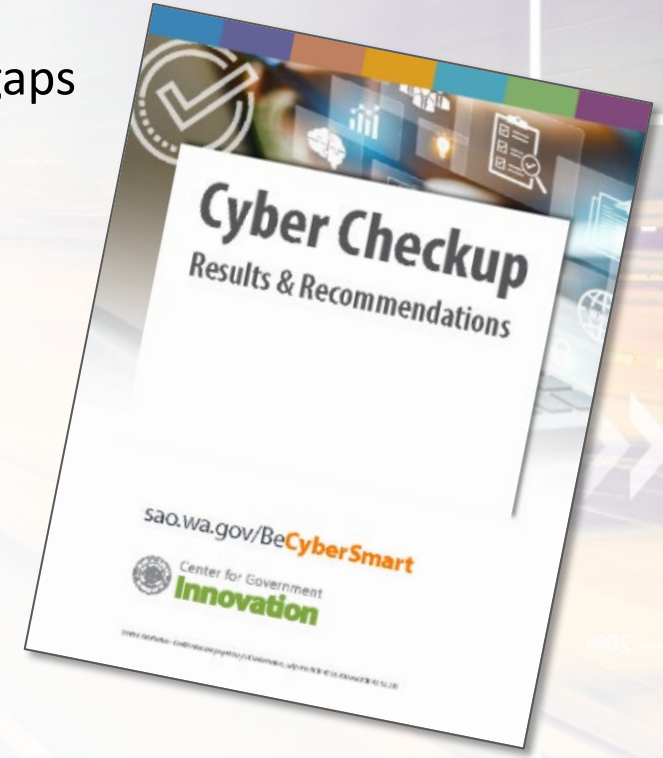


sao.wa.gov/becybersmart/

Introducing Cyber Checkups

The Center's free cyber checkups will help Washington's local governments:

- Understand security safeguards and why they're important
- Begin building a cybersecurity program or strengthen an existing one
- Rank the urgency of identified security gaps and prioritize improvements
- Connect to free and low-cost resources



Checkups are built on the framework of the CIS Controls, Version 8.0

We work with several partner agencies

Washington Technology Solutions (WaTech)

State's primary technology agency, responsible for state-level cybersecurity, including incident response

Military Department

Governor's homeland security advisor, responsible for helping secure critical infrastructure and coordinating statewide emergency responses

Secretary of State's Office

Responsible for elections, protects the statewide Election Management System and the state's Voter Registration database

State Auditor's Office

Conducts independent cybersecurity audits of state agencies and local governments, provides cybersecurity resources for local governments, plus trainings, presentations and consultations

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

Website: www.sao.wa.gov
Twitter: @WAStateAuditor
Facebook: WaStateAuditorsOffice
LinkedIn: Washington State Auditor's Office

Office of the Washington State Auditor
Pat McCarthy