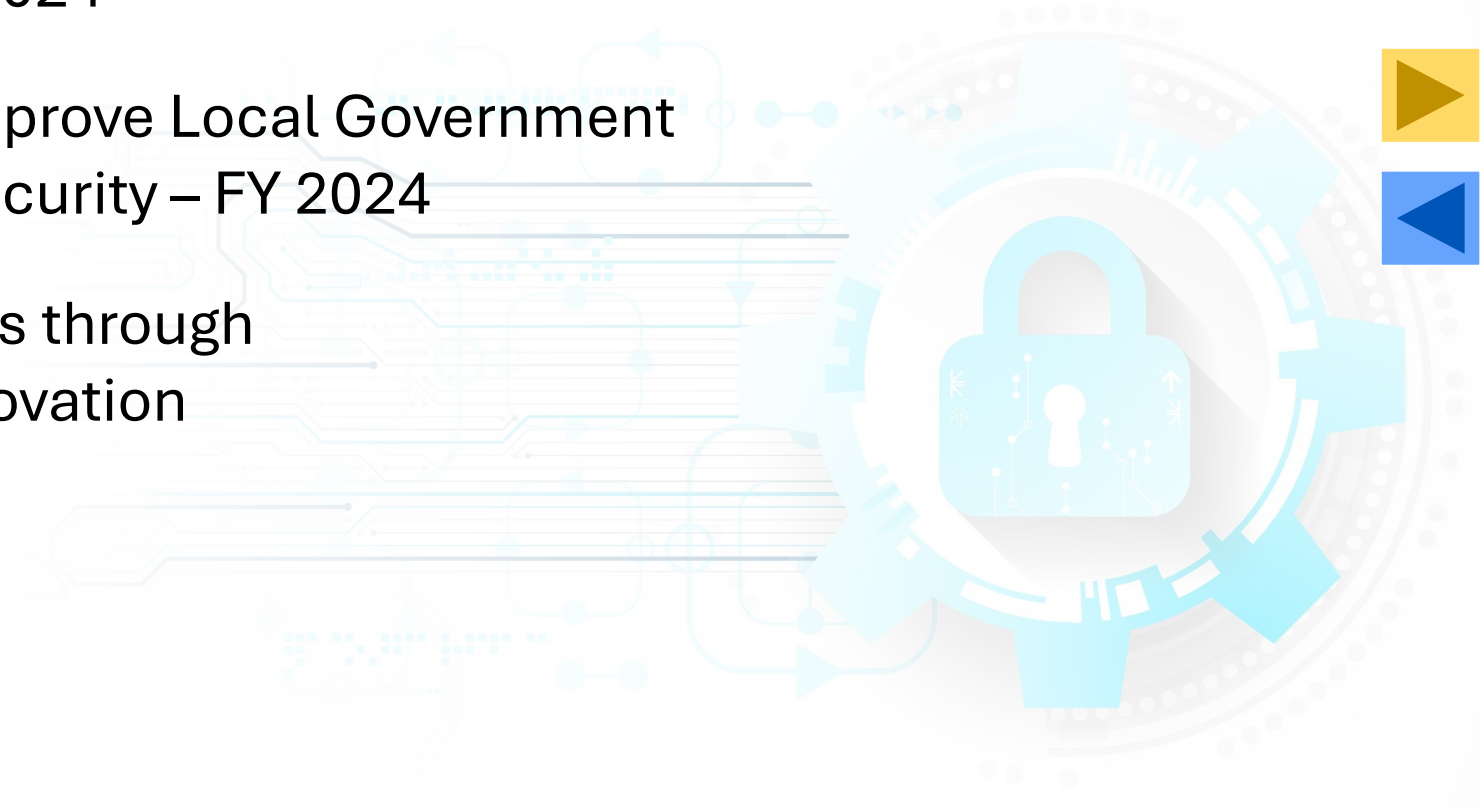
State Auditor's Office Cybersecurity Update Fiscal Year 2024

For reports published September 9, 2024

Topics in this year's rollup report

- State Auditor's Office portfolio of cybersecurity efforts
- Continuing Opportunities to Improve State Agency IT Security Organizations – FY 2024
- Continuing Opportunities to Improve Local Government and Critical Infrastructure IT Security – FY 2024
- Award-winning Cyber Checkups through the Center for Government Innovation



Continuing to expand our audit reach

Type of audit	Who is served	Total completed	Year started	In this report period
Cybersecurity	State agencies	39	2013	5
Cybersecurity	Local governments	54	2013	8
Critical infrastructure	Local governments	44	2022	12
Ransomware resiliency	Local governments	3	2023	3
Cyber checkups	Local governments	50+	2023	42

Cybersecurity performance audits underway at:

- 7 state agencies, 12 local governments,
  10 critical infrastructure local governments

Delivery of detailed 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

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;

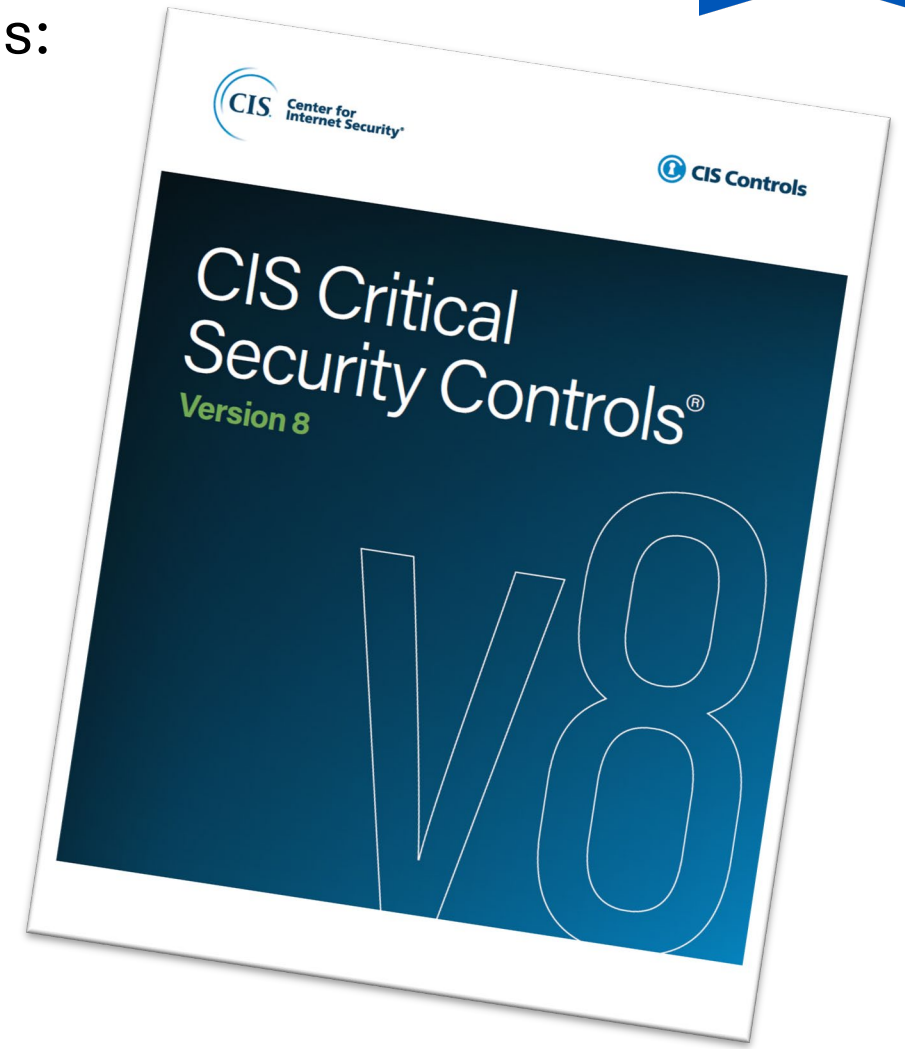
Opportunities to Improve IT Security at State Agencies – FY2024

Audit work completed in FY 2024 at five state agencies

State agency cybersecurity audits

Audits include assessments work in two areas:

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



State cybersecurity **safeguard** results

- Scope based on size, maturity and specific concerns or efforts of each agency, but with higher baseline than local governments
- 168 total safeguards assessed across five agencies
- Assessed an average of 34 safeguards at each government, out of 153 possible elements

61%

Implementation				
All devices	**Most devices**	**Some devices**	**Partially**	**Not in place**
52	21	29	43	23
31%	13%	17%	26%	14%

State cybersecurity **penetration test** results

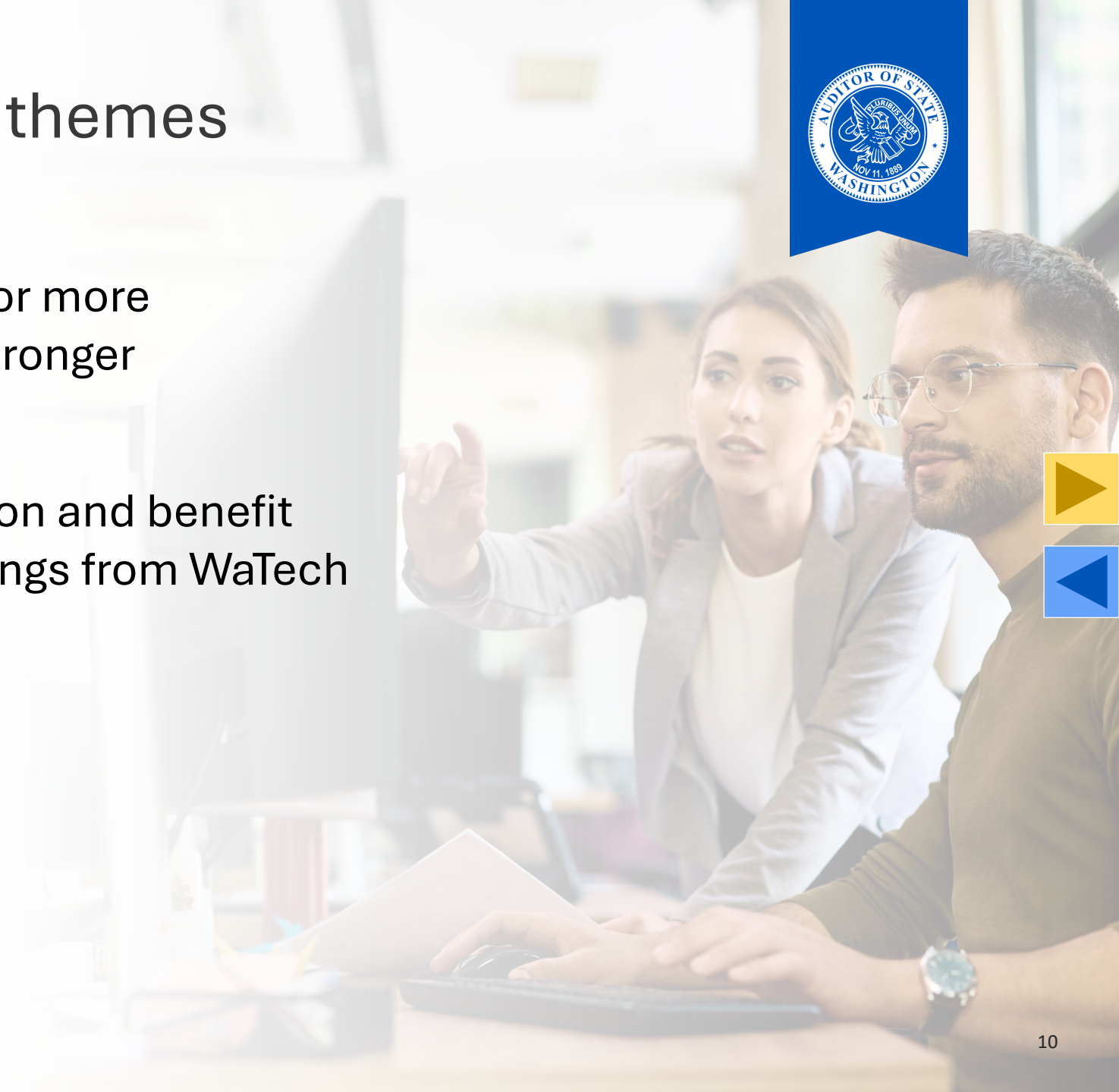
- Across these five state agencies, penetration testing was conducted on 27 applications and various network segments
- Identified 188 vulnerabilities of the following severity levels:

Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
1	**26**	29	81	51	188

- The **27** most severe vulnerabilities could more readily be exploited by hackers to cause a security breach

Common state agency themes

- Agencies that have more staff or more consistent staff tend to have stronger security controls
- Agencies increasingly depend on and benefit from centralized security offerings from WaTech



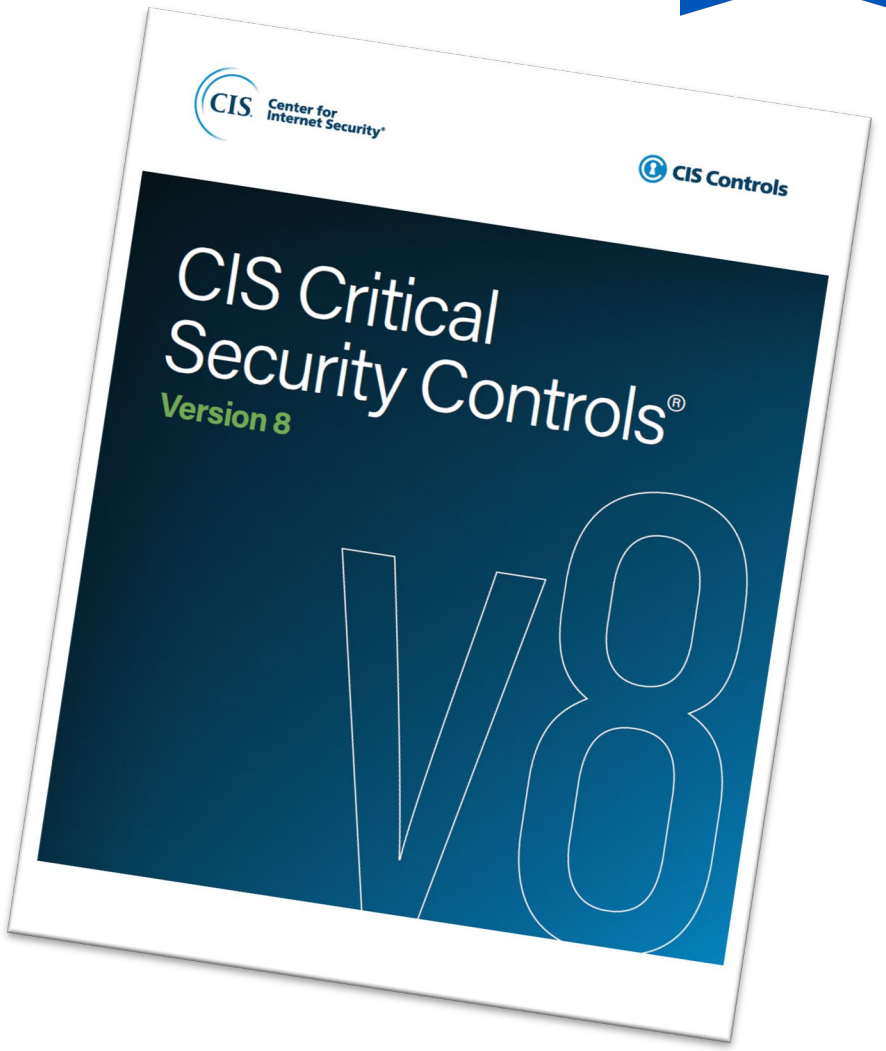
Opportunities to Improve IT Security at Local Governments – FY2024

Audit work completed in FY 2024 at 23 total local governments

- Eight cybersecurity audits
- Three ransomware resiliency audits
- Twelve critical infrastructure audits

Local cybersecurity audits

- Completed during the fiscal year at eight 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



Local cybersecurity **safeguard** results

- 258 total safeguards assessed across eight governments
- Assessed an average of 32 safeguards at each government, out of 153 possible elements
- Scope based on size, maturity and specific concerns or efforts of each government

53%

Implementation				
All devices	**Most devices**	**Some devices**	**Partially**	**Not in place**
63	45	30	85	35
24%	17%	12%	33%	14%

Local cybersecurity **penetration test** results

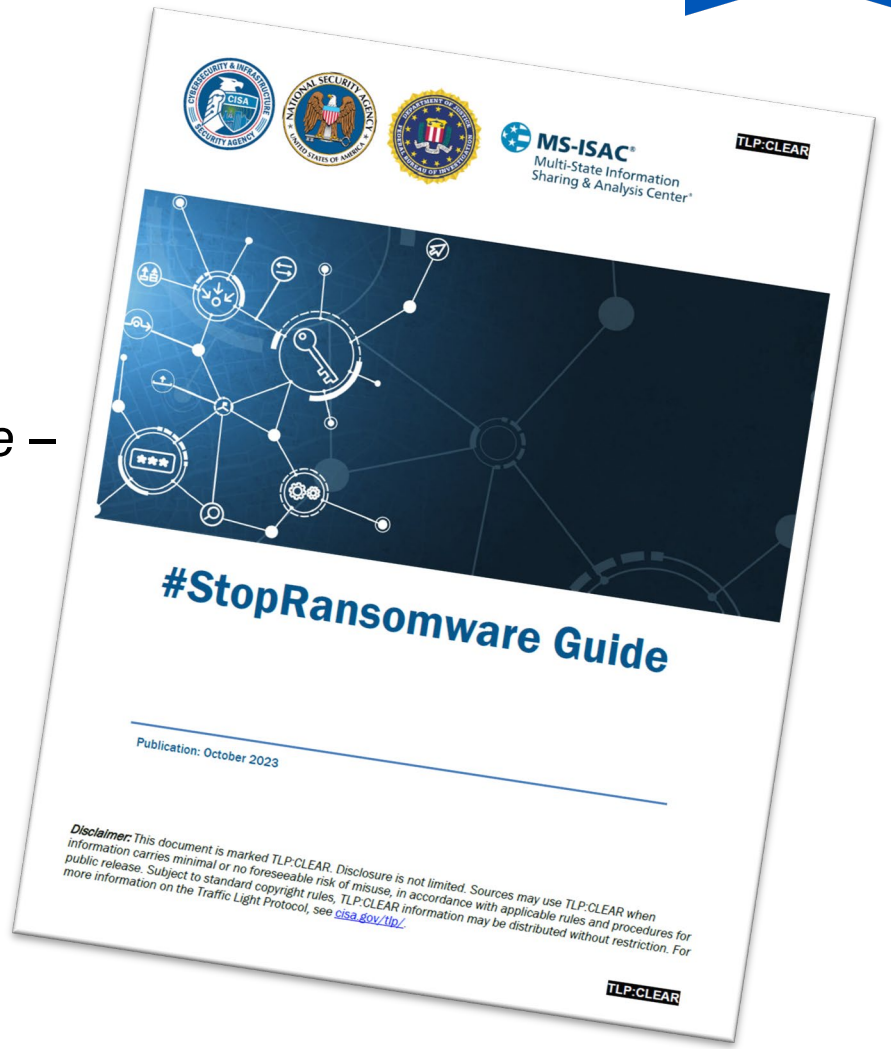
- Across these eight local governments, penetration testing was conducted on 35 applications and various network segments
- Identified nearly 300 vulnerabilities of the following severity levels:

Severity					
Critical	**High**	Medium	Low	Informational & observations	**Total**
4	**66**	48	111	57	286

- The **70** most severe vulnerabilities could more readily be exploited by hackers to cause a security breach

Ransomware resiliency audits

- Completed during the fiscal year at 3 local governments
- Included assessment work in two areas:
  - ✓ Compared local government practices to recommendations from *Stop Ransomware* – Joint Ransomware Task Force
  - ✓ Performed vulnerability and technical analysis tied to assessed best practices using Auditor's Office staff and tools



Ransomware resiliency audit results

- Assessed the same 22 safeguards at each of the 3 governments for 66 total
- 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

30%

Implementation		
Fully in place	**Partially**	**Not in place**
20	32	14
30%	49%	21%

Critical infrastructure audits

Focused on local governments providing critical infrastructure, such as water, sewer, energy 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 12 local governments with critical infrastructure
  - Includes 10 water and/or sewer providers, which aligns with federal and state priorities introduced earlier this year
- Includes high-level review of IT practices
- Primary focus on external penetration testing
- Identified 75 vulnerabilities, with the following severity levels:

Severity					
Critical	High	Medium	Low	Informational & observations	**Total**
0	10	9	33	23	75

Common themes at audited local governments

- Greater focus on cybersecurity overall
- Governments undergoing a repeat audit and those with dedicated IT security staff had best implementation results
- Cybersecurity elsewhere is inconsistent. No strong correlation between good implementation and IT staffing methods, such as:
  - No IT staff
  - Part-time IT staff
  - Vendor-only IT support
  - Small IT department without IT security staff

Center for Government Innovation #BeCyberSmart Program

The Center for Government Innovation's cybersecurity program offers:

- Resources
- Training
- Presentations
- Technical advice
- Cyber Checkups

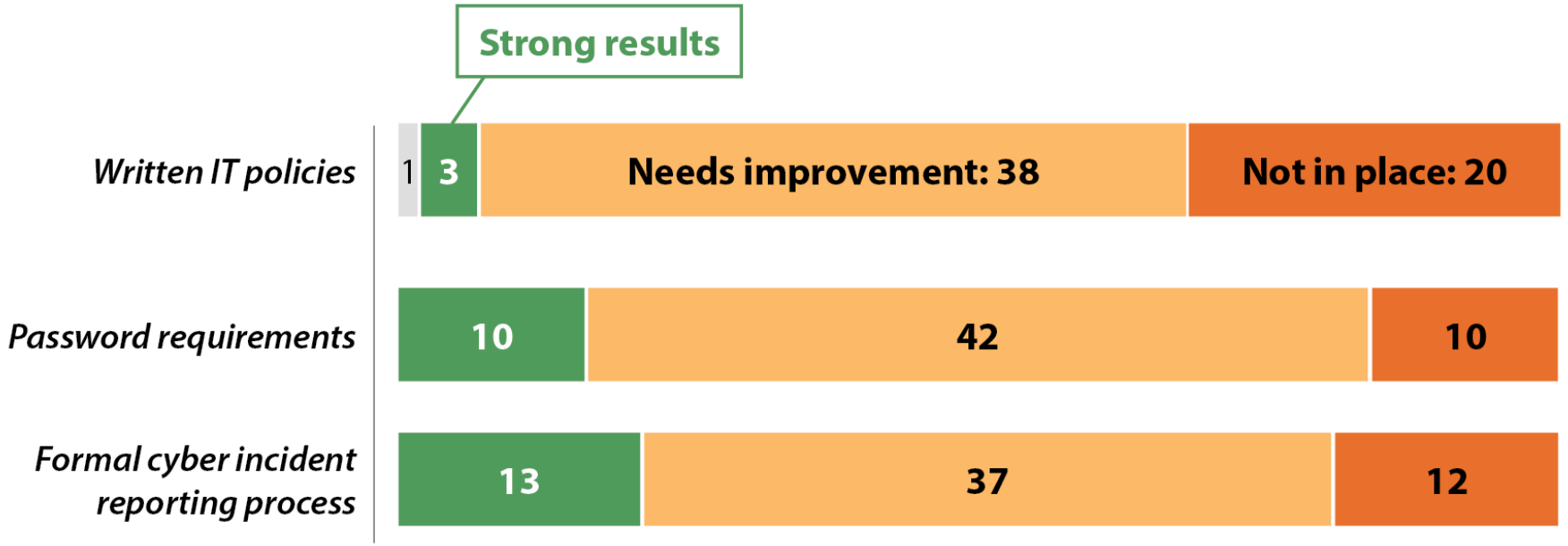
sao.wa.gov/becybersmart/

Award-winning Cyber Checkups

- Winner of 2024 NSAA Excellence in Accountability Special Projects award
- Completed 62 checkups since program began in 2023
- The Center's free cyber checkups are suitable for governments without IT departments and help 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

Cyber checkup results

- Completed checkups at 62 local governments since program began in 2023
- Cyber checkups cover 20 topic areas, with results ranked as *strong*, in *need of improvement* or *not implemented*



Additional resources, audits and coordination from our Office

- Newest resource for local governments: *It starts with policy – a guide to jump-starting your cybersecurity program*
- Security attestation engagements (WaTech and Department of Licensing)
- Cyber loss follow-up

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
X: @WAStateAuditor
Facebook: www.facebook.com/WaStateAuditorsOffice
LinkedIn: Washington State Auditor's Office