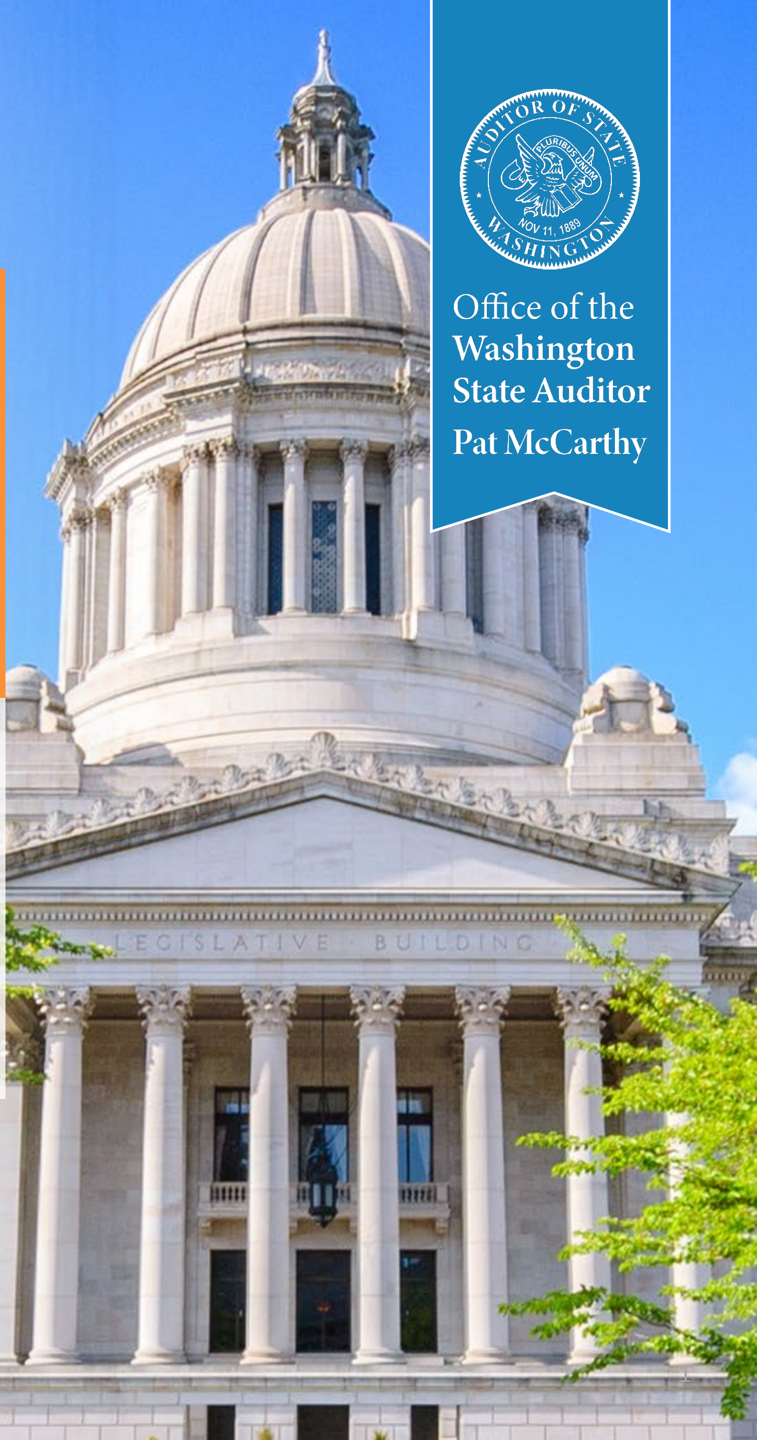
Office of the Washington State Auditor
Pat McCarthy

Continued Cybersecurity Efforts at the State Auditor's Office

Joe Clark, *IT Security Assistant Audit Manager*
Clyde-Emmanuel Meador, *IT Auditor*

Joint Legislative Audit & Review Committee
January 6, 2021

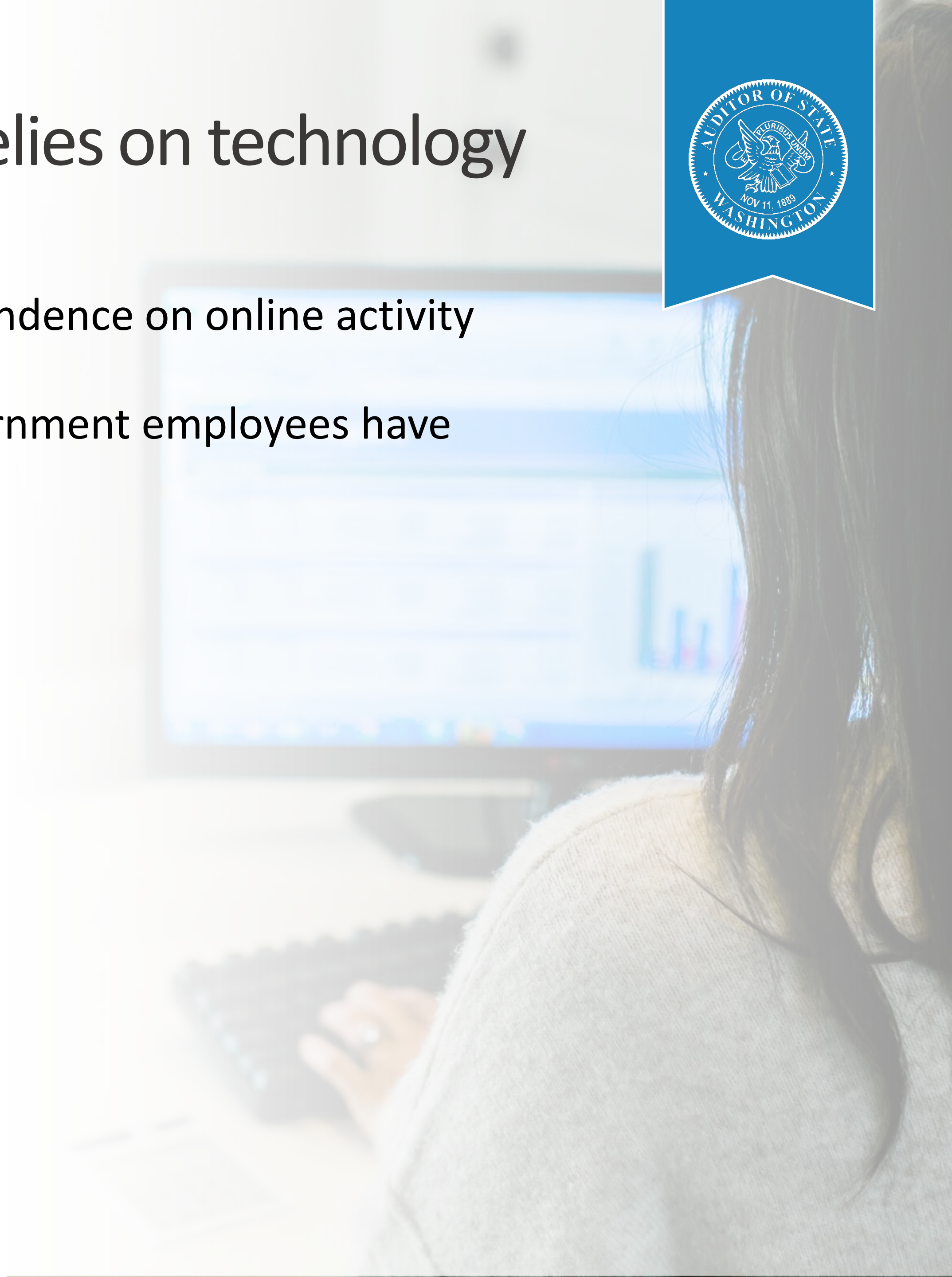


Agenda for today’s presentation

- Continued importance of cybersecurity
- Cyber threats facing state and local governments
- State Auditor’s Office cybersecurity portfolio
- 2020 State cybersecurity audit presentation

Society increasingly relies on technology

- COVID-19 has increased dependence on online activity
- Since March 2020, state government employees have worked primarily from home



Cybersecurity is as important as ever to the state

- Supporting a remote workforce places additional burdens on IT staff

- Remote working has also changed the attack landscape, offering hackers new opportunities

- Protecting state systems and data requires additional vigilance

Washington has already been targeted

Attacks against federal, state and local governments are common

- Washington state attacked in September 2020

The Office of Cybersecurity responded

- Adapted and implemented additional strategies to protect state systems from future attacks

Our Office’s cybersecurity efforts

In addition to audits, our portfolio of cybersecurity activities include non-audit offerings:

- ✓ Cybersecurity consultations
- ✓ #BeCyberSmart Campaign
- ✓ Ongoing coordination with stakeholders

#BeCyberSmart Campaign

- Curated suite of cybersecurity resources for local government
- Customized by role in government
- Designed as a place for governments to start

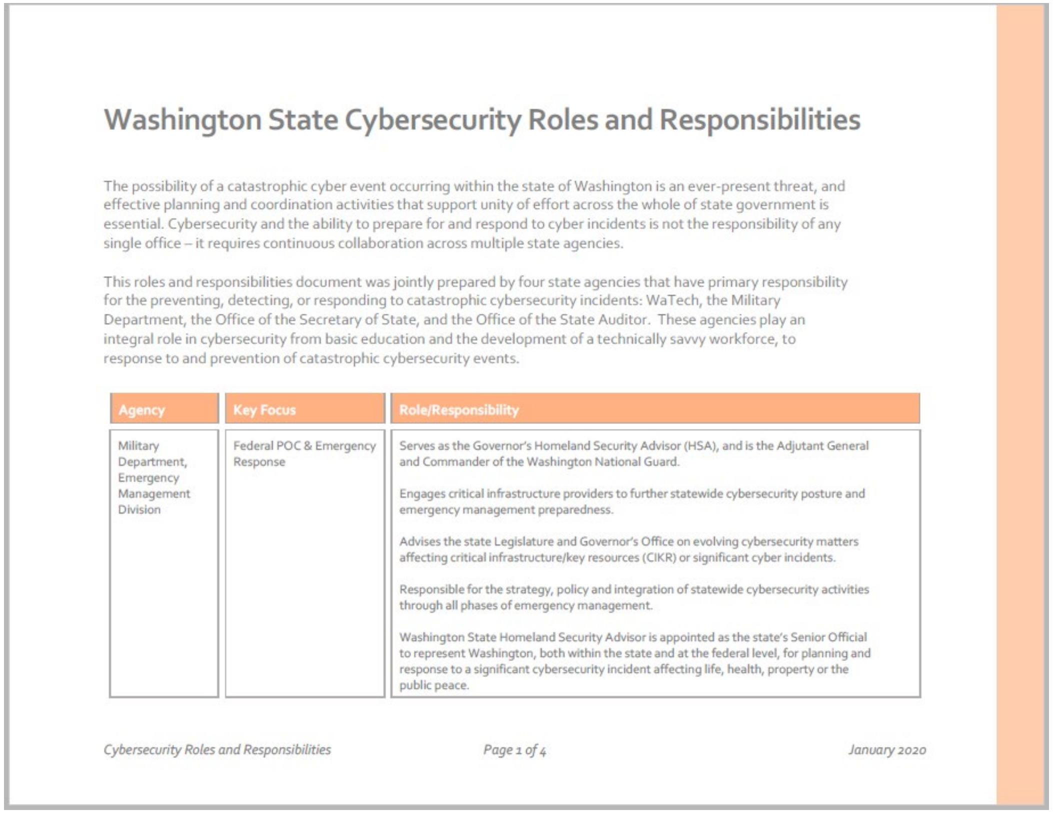
www.sao.wa.gov/becybersmart/

Coordination with stakeholders

Office of the Washington State Auditor

Pat McCarthy

- Monthly meetings with the Office of Cybersecurity to coordinate on cybersecurity and IT audits
- Semi-annual meetings with other agencies to coordinate cyber responsibilities



Washington State Cybersecurity Roles and Responsibilities

The possibility of a catastrophic cyber event occurring within the state of Washington is an ever-present threat, and effective planning and coordination activities that support unity of effort across the whole of state government is essential. Cybersecurity and the ability to prepare for and respond to cyber incidents is not the responsibility of any single office – it requires continuous collaboration across multiple state agencies.

This roles and responsibilities document was jointly prepared by four state agencies that have primary responsibility for the preventing, detecting, or responding to catastrophic cybersecurity incidents: WaTech, the Military Department, the Office of the Secretary of State, and the Office of the State Auditor. These agencies play an integral role in cybersecurity from basic education and the development of a technically savvy workforce, to response to and prevention of catastrophic cybersecurity events.

Agency	Key Focus	Role/Responsibility
Military Department, Emergency Management Division	Federal POC & Emergency Response	Serves as the Governor's Homeland Security Advisor (HSA), and is the Adjutant General and Commander of the Washington National Guard. Engages critical infrastructure providers to further statewide cybersecurity posture and emergency management preparedness. Advises the state Legislature and Governor's Office on evolving cybersecurity matters affecting critical infrastructure/key resources (CIKR) or significant cyber incidents. Responsible for the strategy, policy and integration of statewide cybersecurity activities through all phases of emergency management. Washington State Homeland Security Advisor is appointed as the state's Senior Official to represent Washington, both within the state and at the federal level, for planning and response to a significant cybersecurity incident affecting life, health, property or the public peace.

Cybersecurity Roles and Responsibilities *Page 1 of 4* *January 2020*

Cybersecurity audits

Cybersecurity performance audits

- ✓ State agencies
- ✓ Local governments

To date, SAO has completed audits of:

- ✓ 22 unique state agencies
  - ○ Plan to audit at least five agencies in 2021
- ✓ 21 local governments
  - ○ Nine more underway

Opportunities to improve state IT security – 2020

State agencies have unique IT security challenges

- Must protect systems and data, required by Office of the Chief Information Officer's Standard 141.10

- Must provide services:
  - ✓ Across wide geographic areas
  - ✓ To large numbers of people
  - ✓ Using internet-based web portals

Auditors look for opportunities for agencies to improve their IT security practices

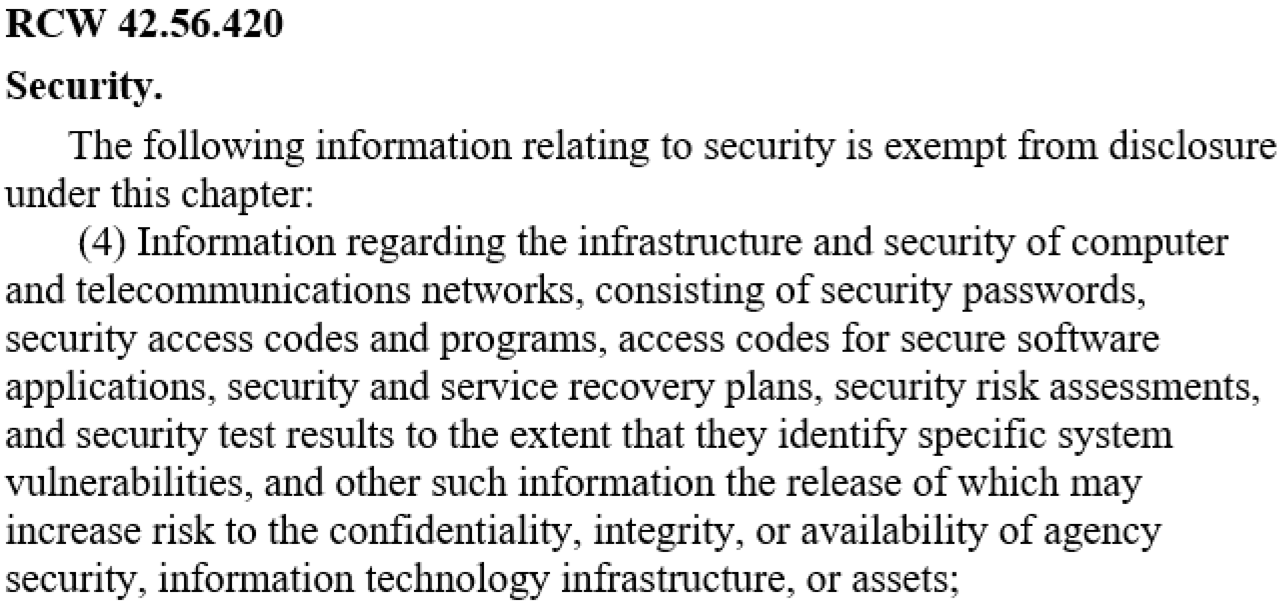
Audit overview – Cyber 6

2020 cybersecurity performance audit of selected state agencies

- One large agency, two medium agencies, and two small agencies
- Sixth in this series of audits, covering 22 individual agencies
- Assessed network and application security and IT security practices

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;

Can selected agencies make their IT systems more secure?

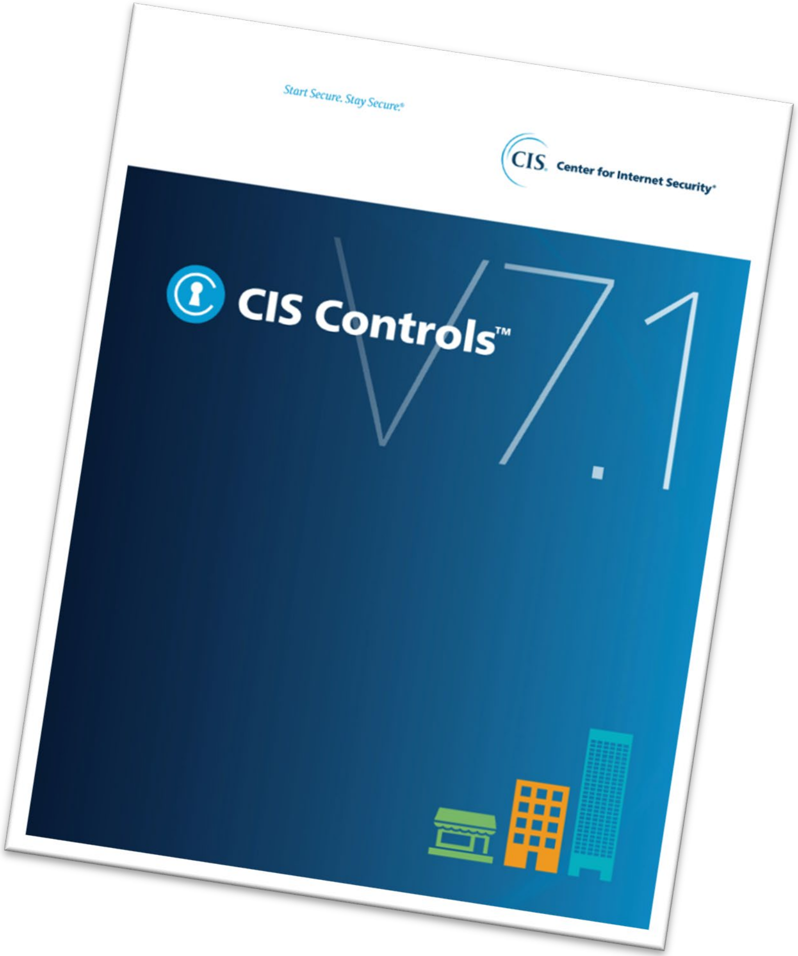
- Penetration testing of one agency's network and applications
  - ✓ External
  - ✓ Internal
- Performed by contracted subject matter experts
- Due to COVID-19, most penetration testing was delayed into 2021

Can they better align their IT security practices with leading practices?

- Compared agency practices to controls from the Center for Internet Security

✓ Informed by private- and public-sector stakeholders

✓ Prioritize benefits



Start Secure. Stay Secure.

CIS. Center for Internet Security

CIS Controls™

V7.1

The CIS Controls we considered

1. Inventory and control of hardware assets
2. Inventory and control of software assets
3. Continuous vulnerability management
4. Controlled use of administrative privileges
5. Secure configurations for hardware and software
6. Maintenance, monitoring and analysis of audit logs

11. Secure configuration for network devices, such as firewalls, routers and switches

Results overview

We found strengths in agencies' security

- ✓ Some agencies had robust vulnerability management programs
- ✓ Two agencies leveraged versatile technical tools and built business processes to address risk in multiple control areas

Results overview

Agencies could use the CIS Controls to further improve security

- ✓ Although all five agencies had patch management processes, two did not have vulnerability scanners
- ✓ Documenting IT security practices helps prioritize security activities and preserve institutional knowledge

Factors that contributed to performance results

- All five agencies reported resource availability as a notable factor in implementing IT security controls

  ✓ Four of five agencies told us that retaining or employing sufficient qualified staff was a challenge

- Two agencies reported highly qualified IT security staff were key to their success

Recommendations

We recommend the five state agencies:

- Further align agency IT security controls with leading practices recommended in the CIS Controls
- Identify and continue to periodically assess IT security needs and resources, including personnel and technology
- Prioritize and continue remediating vulnerabilities identified during security testing

Questions

Contact Information

Pat McCarthy

State Auditor

Pat.McCarthy@sao.wa.gov

(564) 999-0801

Scott Frank

Director of Performance & IT Audit

Scott.Frank@sao.wa.gov

(564) 999-0809

Joseph Clark

IT Security Assistant Audit Manager

Joseph.Clark@sao.wa.gov

(564) 999-0968

Clyde-Emmanuel Meador

IT Auditor

Clyde-Emmanuel.Meador@sao.wa.gov

(564) 999-0971

Website: www.sao.wa.gov

Twitter: www.twitter.com/WaStateAuditor

Facebook: www.facebook.com/WaStateAuditorsOffice