

Cybersecurity Auditing in Washington State

Western Intergovernmental Audit Forum

Scott Frank, Director of Performance and IT Audit
Peg Bodin, Assistant Director of IT Audit

October 29, 2019



Office of the
Washington
State Auditor
Pat McCarthy

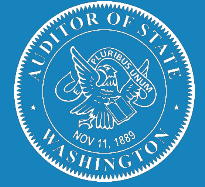


Road Map for Today's Session

- SAO's Mission and Strategic Goals
- Cybersecurity Audits
- Other Cybersecurity Assistance
- PSA: Cyberfraud and ACH Payments
- Wrap Up and Questions



SAO's Mission and Strategic Goals



History of Office



11th State Auditor
Pat McCarthy

*Established in state Constitution
in 1889*



*“We are the public’s window into government.
We take that responsibility seriously, and we
work with the organizations we audit to
increase the public’s trust in government.”*



**Independently
Elected Auditor**

SAO audits every government in the state



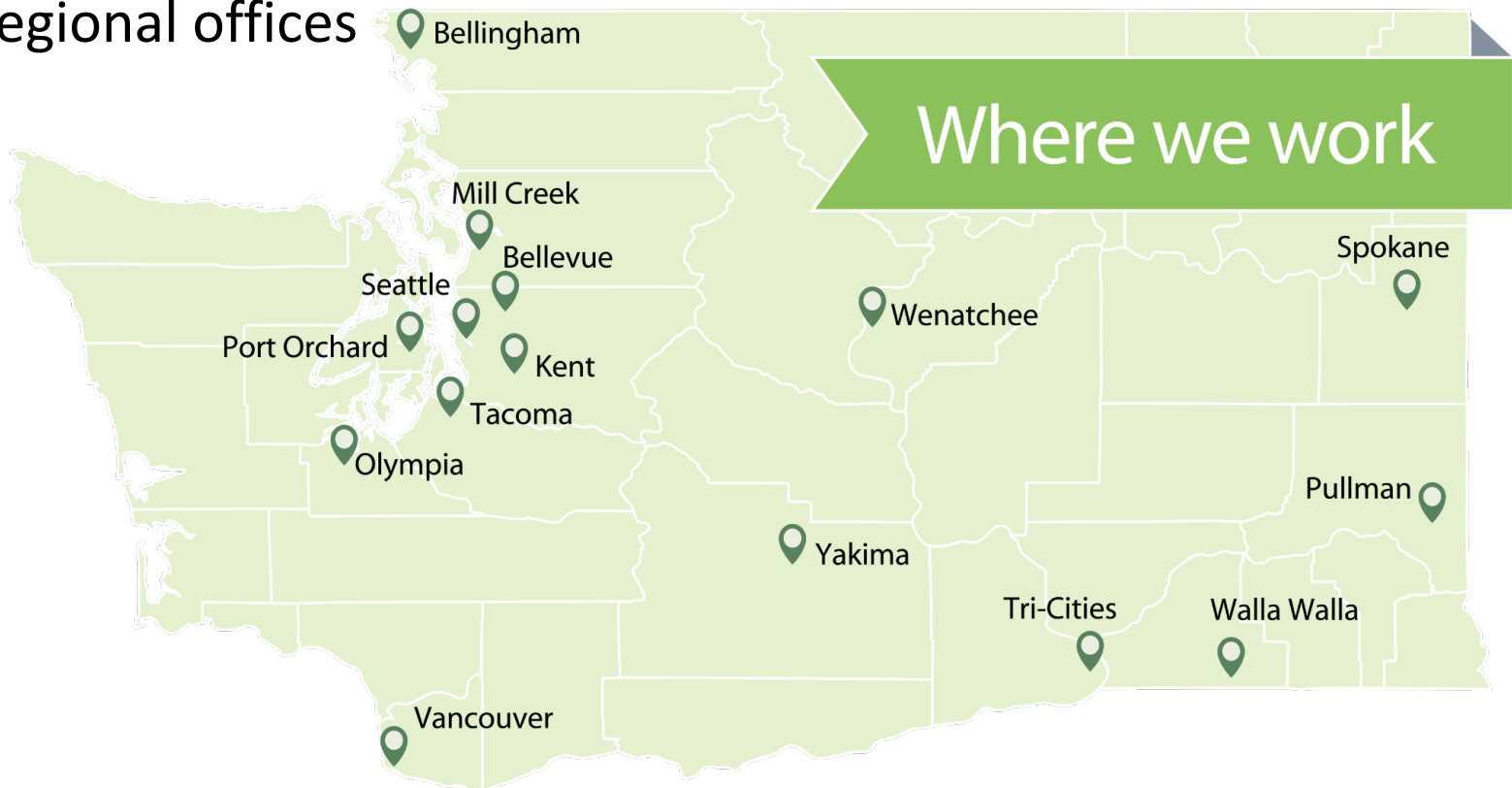
~ **2,300**
local governments

- Includes school districts, library districts, diking and drainage districts, and many others
- We also audit state agencies, such as Department of Social and Health Services as well as universities and community colleges
- In addition, we audit the finances of the state as a whole

Locations and Staff



- 350 auditors
- 15 regional offices





SAO's 5 Strategic Goals

#1: Inform, educate
and empower
public and

#2: Assist state and
local governments to
accountable

Cybersecurity
Help protect the state's confidential
information, financial assets, and
critical infrastructure by improving the
security of state agencies and local
governmental entities.

#5: Ensure
and cost-
operations
continuous
improvement

develop,
retain a
talented
workforce

implement strategies
that promote high
quality audits

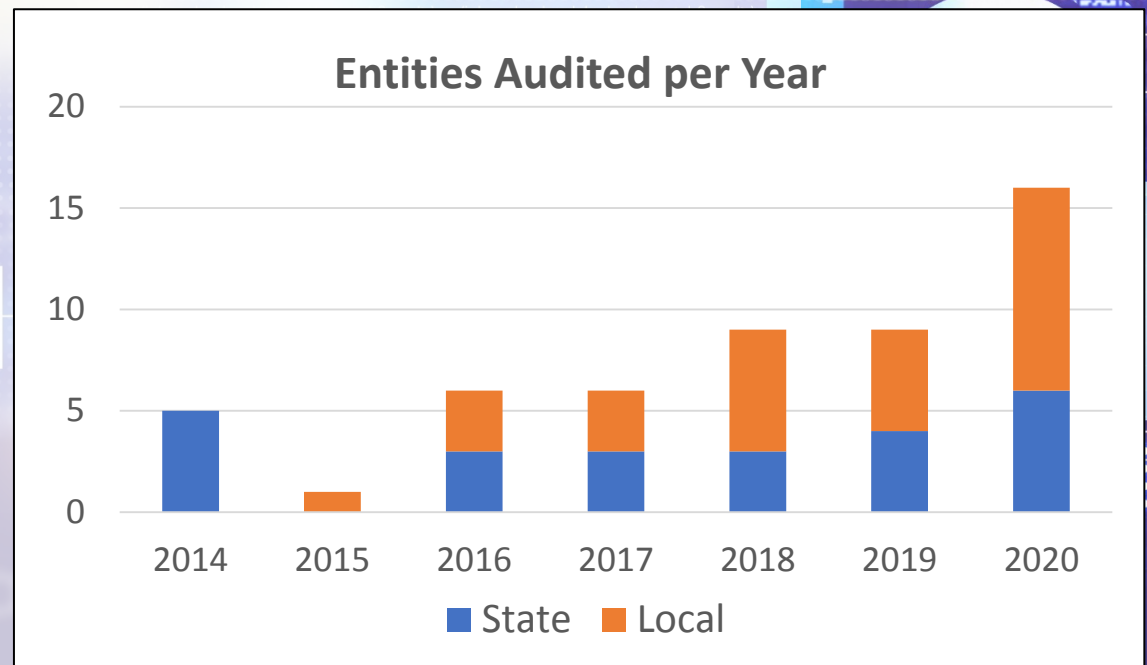
Cybersecurity Audits





Background on Cybersecurity Audits

- Contracted support
- Cybersecurity specialist team
- Consultations
- Additional funding
- Dynamic scoping
- #BeCyberSmart



Our cybersecurity team

- 9 cybersecurity auditors
- 5 cybersecurity specialists
- 1 contractor



Goal and Objectives

Help government make significant cybersecurity improvements

- ✓ Objective 1: Identify weaknesses (vulnerabilities) that could lead to increased risk from external or internal threats.
- ✓ Objective 2: Selected controls aligned with leading cybersecurity practices



Office of the
Washington
State Auditor
Pat McCarthy



Identifying Vulnerabilities

- **Vulnerability Assessments**
 - ✓ Primarily automated
 - ✓ Requires some expertise
 - ✓ Red flags – things that need to be evaluated
- **Penetration Testing**
 - ✓ Some automation but requires manual effort
 - ✓ Requires more expertise
 - ✓ Confirmed issues – things that need to be fixed



Leading Practice: NIST 800-53 Security and Privacy Controls for Federal Information Systems

- Federal government
- Policy / governance
- Comprehensive scope
- Control selection based on risk



Leading Practice: Center for Internet Security Critical Security Controls

- Not industry specific
- Prioritized set of actions
- Mitigate most common attacks
- Based on community of IT experts
- Technical controls and policies



Dynamic Scoping

Actionable recommendations that will make a difference

Challenges

- One size fits all
- Resources
- Effective results

Scoping Factors

- Current security maturity
- Prioritization of effective recommendations



How Much Should You Report?

- Detailed, confidential results
- Low detail public reports
- Legislative communication



Office of the
Washington
State Auditor



Other Cybersecurity Assistance



More Demand Than We Can Meet



- More than 2,300 local governments in Washington
- Cybersecurity audits at 10-12 locals a year
- Currently about a five-year wait for an audit
- Need some other ways to help
 - ✓ #BeCyberSmart campaign
 - ✓ Cybersecurity Consultations

#BeCyberSmart Campaign



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

#BeCyberSmart Campaign



Office of the
Washington
State Auditor
Pat McCarthy



Leadership and Planning

1. Include cyber-risks when performing entity-wide risk assessments
2. Develop and maintain policies and standards for your organization related to cybersecurity
3. Adequately fund cybersecurity



Facilities and Operations

1. Identify cyber-risks to infrastructure
2. Ensure facilities have appropriate security controls
3. Improve security of infrastructure using cybersecurity best practices



Finance and Administration

1. Fund cybersecurity to enable its success
2. Work with other departments to ensure third party contracts include appropriate cybersecurity accountability clauses
3. Protect sensitive financial, legal and other confidential information



Legal and Compliance

1. Educate yourself on the legal implications of cybersecurity
2. Implement an effective compliance program
3. Actively work across teams to create a holistic risk mitigation plan



Information Technology

1. Create a robust cybersecurity program
2. Integrate security into design, architecture, deployment, and routine operations
3. Maintain excellent technical competence in cybersecurity



Human Resources

1. Train employees on cybersecurity
2. Evaluate and support staffing needs to address cyber-risks
3. Protect access to sensitive employee information through cybersecurity best practices



CYBERSECURITY
is everyone's job.



Finance and
Administration

Finance matters

Considerations extend beyond
budget decisions

As a finance or administrative professional in a local government, you have key responsibilities for managing that government's resources. In your role, you interact with all aspects of a local government's operations as you inform budgetary decisions.

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



Office of the Washington State Auditor
Pat McCart

Last updated August

You have an essential role to play in keeping your government cyber-secure, through ensuring adequate funding of cybersecurity, addressing cyber-risks in the budget and within contracts, and keeping confidential information housed in financial management software secure.

1 Fund cybersecurity to enable its success

Preparing the budget requires you to consider many competing priorities and help make recommendations on how to spend limited resources. To help balance these demands in your local government, you should participate in an entity-wide risk assessment that also considers cybersecurity risks. The risk assessment can provide actionable information that can help you, as the finance professional, guide the government's leadership in prioritizing and balancing efforts to achieve operational goals and protect from risks.

A risk assessment can be an important tool to make budget recommendations based on the government's needs and priorities consistent with the direction of elected officials.

You can find more information on entity-wide risk assessments in the "Leadership and Planning" section of our #BeCyberSmart webpage.

Budget considerations include adequately funding cybersecurity. Also, make sure you gain an understanding of what cybersecurity investments your government has already made. This can help you recommend more effective areas for investment.

Additionally, consider training and awareness programs for all staff as part of funding your government's cybersecurity efforts. You should also consider software tools and training needs for IT staff as well as replacement costs for older, unsupported systems that might pose a risk.

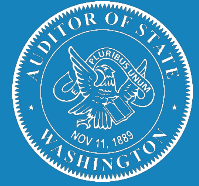
2 Work with other departments to ensure third-party contracts include appropriate cybersecurity accountability clauses

Thinking about cybersecurity for your own local government is difficult, but have you considered all of the risks from third parties you rely on and share information with, such as contractors, vendors and

government partners? These third parties can be a significant source of cybersecurity risk that could affect your government.

Cybersecurity Consultations

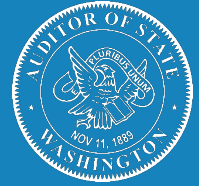
- Short initial meeting with locals who express interest in a cybersecurity audit
 - ✓ 2-4 hours
 - ✓ Within several months of volunteering
- Purpose of the consultation
 - ✓ Begin a relationship with SAO's cybersecurity experts
 - ✓ Gain a general understanding of their security program for future audit planning
 - ✓ Refer them to resources, including #BeCyberSmart



Public Service Announcement: Cyberfraud and ACH Payments



Anatomy of the ACH fraud



Office of the
Washington
State Auditor

Trusted Employee Name
(scammer@gmail.com)



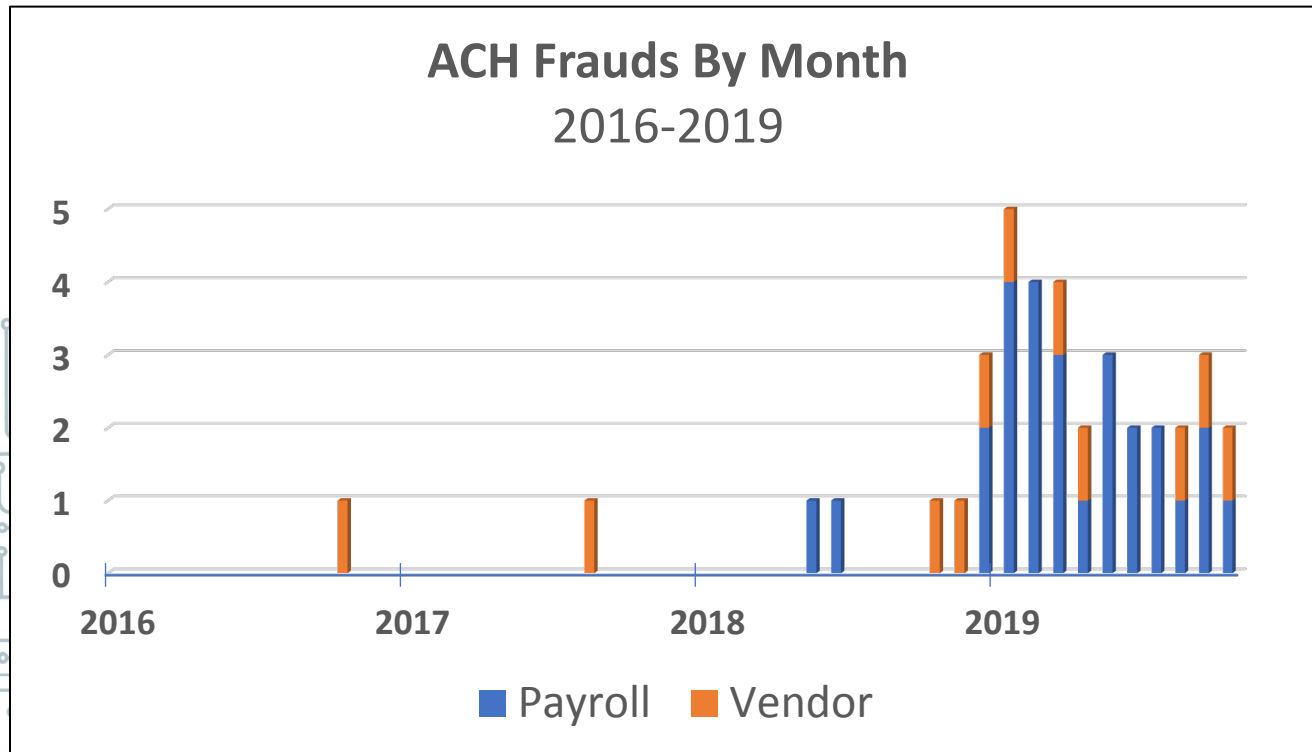
Subject: My Pay Information

Hi,
I would like to change my Direct
Deposit information with my next pay.
Kindly send me the form I need to
submit. What date is the deadline for
submission?

The Challenge: ACH Frauds are Growing



Office of the
Washington
State Auditor



Impact of the frauds



Office of the
Washington
State Auditor

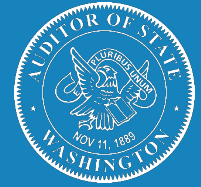
- Payroll ACH (June 2019)
 - ✓ Two payroll periods
 - ✓ Employee reported within 5 days of second missing check
 - ✓ Total Loss: \$8,841
- Vendor ACH (October to November 2018)
 - ✓ Four payments totaling \$220,485
 - ✓ Actual vendor detected
 - ✓ Recovered final payment of \$66,012
 - ✓ Total Loss: \$154,473
- Vendor ACH (March 2019)
 - ✓ Five payments totaling \$6.9 million
 - ✓ Bank detected
 - ✓ Majority of funds recovered
 - ✓ Total Loss: \$118,178



Two Main Ways the Fraud is Initiated

- Social Engineering or Email Spoofing
 - ✓ Trickery
 - ✓ Easily detected
 - ✓ Easily prevented
- System Compromise
 - ✓ Email or network
 - ✓ Risk extends beyond ACH loss
 - ✓ Difficult investigation
 - ✓ Fraud is still easily prevented but...

The High-Tech Solution



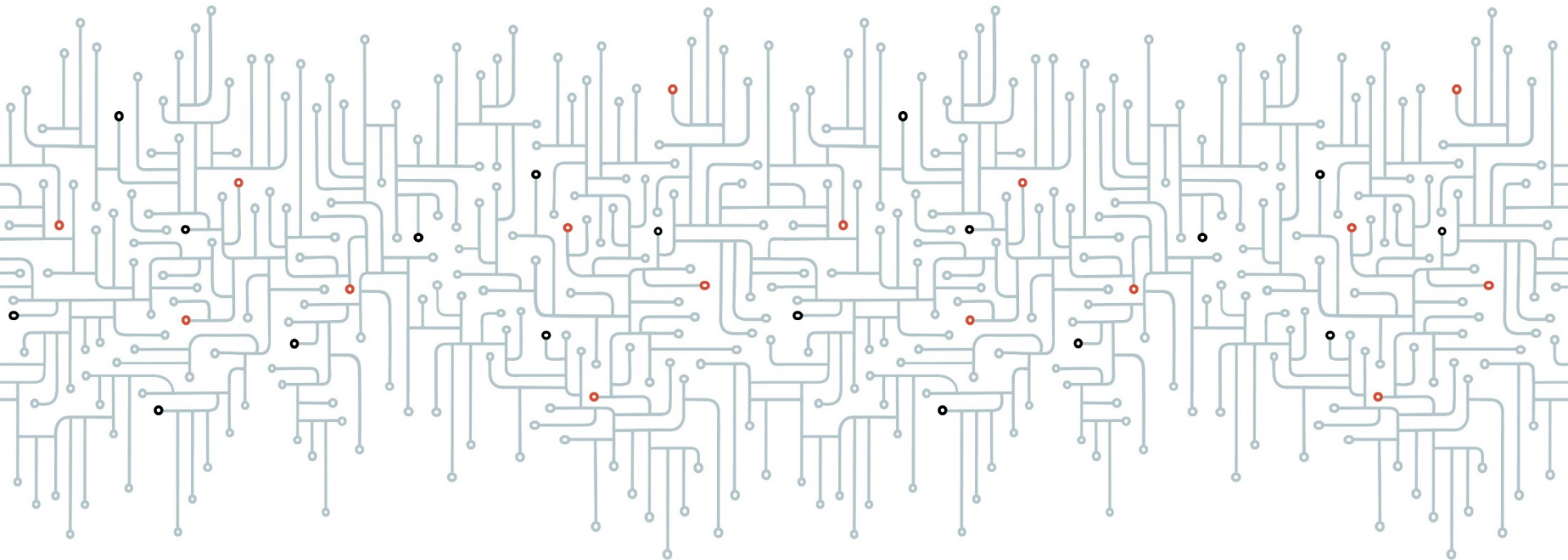
Office of the
Washington
State Auditor



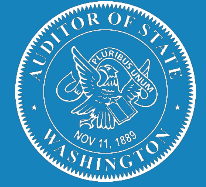
Our Approach to Addressing This



- Get the word out to everyone
- Required risk to assess
- Control-based testing strategy




Final Thoughts



Cybersecurity Audits Help Move the Needle on Security

- Government entities are under attack from hackers
- This isn't going away
- Many government entities lack strong cybersecurity programs
- This is especially true at the local level
- Cybersecurity audits can help government entities improve their security



...the state-led cybersecurity audits are credit positive for Washington local governments because they proactively help identify potential vulnerabilities, giving the municipalities and opportunity to mitigate these threats before they materialize.

--Moody's Investor Service,
August 2018

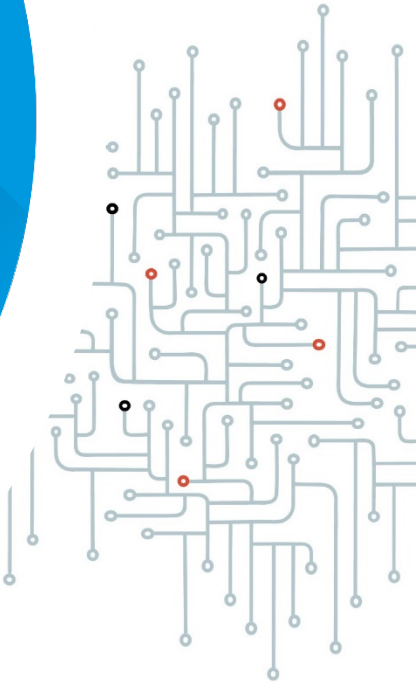
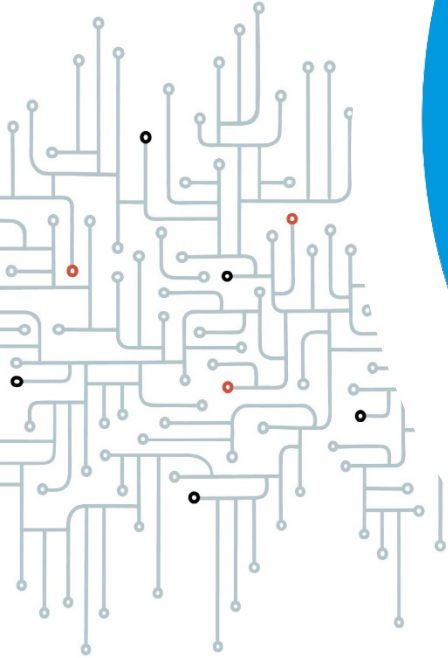


Additional Resources

- Center for Internet Security – CIS Controls
 - ✓ <https://www.cisecurity.org/controls/>
- NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
 - ✓ <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
 - ✓ <https://www.cisecurity.org/ms-isac/>
- SAO's #BeCyberSmart Page
 - ✓ <https://www.sao.wa.gov/becybersmart/>
- SAO's Guidance on ACH Fraud
 - ✓ <https://www.sao.wa.gov/where-are-your-payments-going-this-month/>



Questions



Contact Information



Scott Frank, Director of Performance and IT Audit, Scott.Frank@sao.wa.gov

Peg Bodin, Assistant Director of IT Audit, Peggy.Bodin@sao.wa.gov

Website: www.sao.wa.gov

Twitter: www.twitter.com/WaStateAuditor

Facebook: www.facebook.com/WaStateAuditorsOffice