In the Know with SAO

Updates, Resources and Emerging Issues



Josh Stohr, Port Subject Matter Expert

WPPA Small Ports

October 22, 2026

Agenda

01 What's going on with SAO

02 Resources and guides

03 What's going on with ports

04 Procurement of architecture and engineering

05 Open floor/questions

What's going on with SAO

- How to stay up to date
- Looking back at the last year



About the State Auditor's Office



State Auditor
Pat McCarthy

- Non-audit services
  - Center for Government Innovation
  - Technical support
- Audit services
  - Performance & IT audit
  - State & local audit

Types of audits



Accountability



Use of deadly force



Cybersecurity



Financial



Fraud



Energy



Federal compliance



Whistleblower

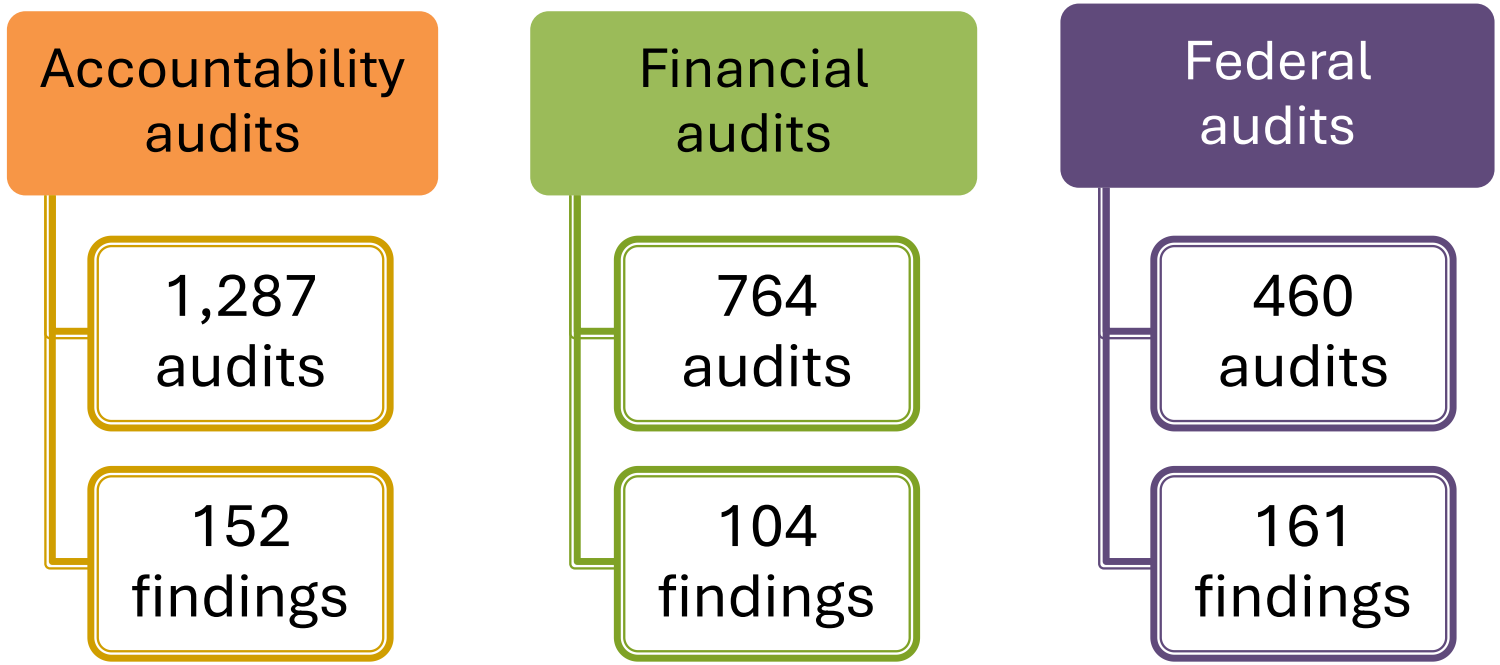


Performance

Audits by the numbers

2,854 audits total

July 1, 2025 – June 30, 2026



Subscribe to SAO's digital resources



Ways to sign up:

1. Via SAO's website at sao.wa.gov
2. Use the QR code below:

SAO Navigator

The SAO Navigator offers regular email reminders throughout the year at the moments that matter most.

- Important deadline reminders
- Practical how-to tips
- Links to useful tools and trainings
- Access to free SAO resources



Resources and guides

- Who can I call with questions?
- SAO's Center for Government Innovation
- Resource Library



SAO support for governments

Governments always have support when work with SAO.

- People you can contact:
  - ✓ Local audit team
  - ✓ Program managers and subject matter experts (SMEs)
  - ✓ Client Help Desk
  - ✓ And more …



The Center for Government Innovation

- **Cyber checkups** to assess your government's vulnerability to common cybersecurity threats
- **Customized Lean facilitations & trainings** to help you improve how work gets done
- **Resource Library** with tools, checklists and other resources that provide you ways to improve internal controls, compliance and other areas
- **Teambuilding workshops** to help you strengthen your team, increase trust and promote workplace harmony
- **Financial Intelligence Tool (FIT)** to help you monitor your government's financial health

A multi-point inspection for a government's cyber program

- Completed remotely
- Answer a 20-question survey about security policies and practical measures
- Identifies cybersecurity gaps and prioritize improvements
- SAO produces a summary of your results and recommendations

Checkups are fast, **free** and confidential

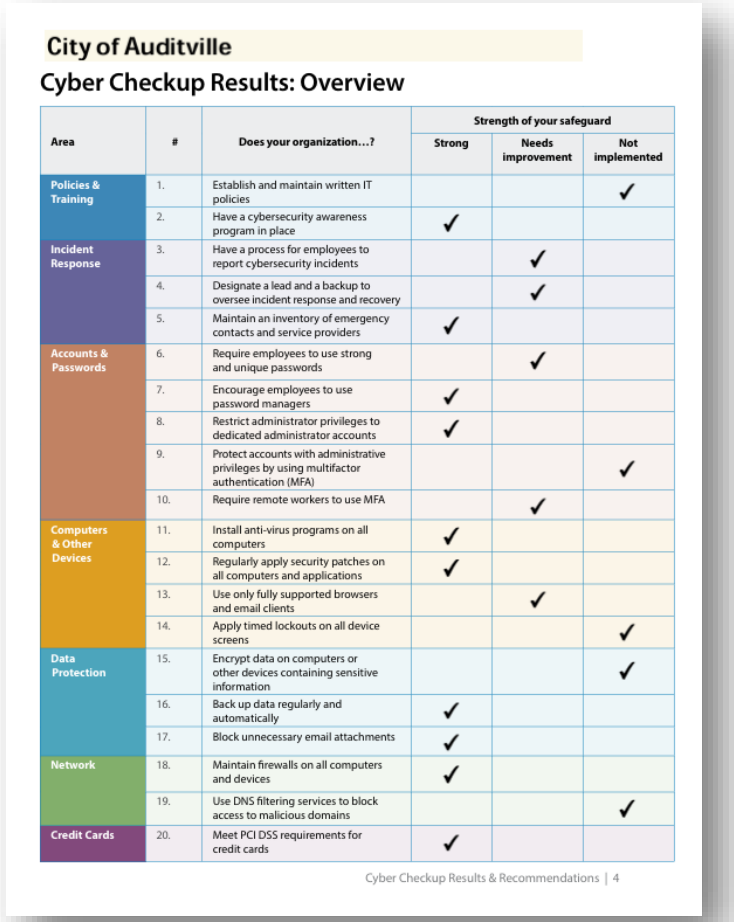


Cyber checkup – what to expect

Five step process:

1. **Questionnaire**: complete a questionnaire about their current cybersecurity practices
2. **Planning meeting**: a cybersecurity specialist meets (remotely) with you (and your team) to discuss questionnaire responses, clarify details, and gather further information
3. **System review**: the cybersecurity specialist conducts a remote review of your IT systems
4. **Checkup results**: you'll receive a confidential report with the results of the evaluation along with detailed recommendations
5. **Final meeting**: the cybersecurity specialist will meet with you and your team to discuss the results and answer your questions

Cyber checkups



City of Auditville

Cyber Checkup Results: Overview

Area	#	Does your organization…?	Strength of your safeguard		
			Strong	Needs improvement	Not implemented
Policies & Training	1.	Establish and maintain written IT policies			✓
	2.	Have a cybersecurity awareness program in place	✓		
Incident Response	3.	Have a process for employees to report cybersecurity incidents		✓	
	4.	Designate a lead and a backup to oversee incident response and recovery		✓	
	5.	Maintain an inventory of emergency contacts and service providers	✓		
Accounts & Passwords	6.	Require employees to use strong and unique passwords		✓	
	7.	Encourage employees to use password managers	✓		
	8.	Restrict administrator privileges to dedicated administrator accounts	✓		
	9.	Protect accounts with administrative privileges by using multifactor authentication (MFA)			✓
	10.	Require remote workers to use MFA		✓	
Computers & Other Devices	11.	Install anti-virus programs on all computers	✓		
	12.	Regularly apply security patches on all computers and applications	✓		
	13.	Use only fully supported browsers and email clients		✓	
	14.	Apply timed lockouts on all device screens			✓
Data Protection	15.	Encrypt data on computers or other devices containing sensitive information			✓
	16.	Back up data regularly and automatically	✓		
	17.	Block unnecessary email attachments	✓		
Network	18.	Maintain firewalls on all computers and devices	✓		
	19.	Use DNS filtering services to block access to malicious domains			✓
Credit Cards	20.	Meet PCI DSS requirements for credit cards	✓		

Cyber Checkup Results & Recommendations | 4



Policies & Training

Safeguard 2: Have a cybersecurity awareness program in place

About this safeguard

A cybersecurity awareness program trains employees to be mindful of cybersecurity risks as they perform their daily tasks. Employees should be aware of common fraud and phishing schemes, as well as basic techniques bad actors use to trick unsuspecting employees.

Why this safeguard is important

People are often an organization's weakest link. Hackers focus on taking advantage of human nature to gain access to your government's networks and sensitive information. Through social engineering techniques like phishing and smishing (using text messages instead of email), they manipulate human behaviors to gain access to login credentials and networks that, if improperly used, could reveal critical data or otherwise harm your government. While you may have put technical solutions in place to reduce the likelihood malicious activities will succeed, your overall security requires an embedded culture of cybersecurity awareness to be truly effective. With regular training, people can become your government's first line of defense.

What we observed during the checkup

Your organization has a cybersecurity awareness program in place.

Our recommendations

- Develop and implement a policy requiring employees to take regular cybersecurity awareness training. You can find links to example policies in the Resources section below.
- Create a cybersecurity awareness program that fits your government's needs. Awareness encompasses everything from a formal security awareness training program to a monthly email with cybersecurity tips, each designed to influence employees' behavior. There are many low-cost and free resources (see Resources below) to help you get started. You'll find tools for delivering training modules, assessments, and newsletters to keep employees engaged.
- Conduct training as part of onboarding for new employees and then annually for all staff.
- Review your training program and its associated policy annually to ensure your program is keeping up with evolving types of cyberattacks.

Resources and references you can use

- The National Institute of Standards and Technology (NIST) provides a sample template you can use to develop your own security awareness training policy.
- SAO's "People matter in cybersecurity" offers advice for starting an awareness program.
- Infosec Institute offers a free toolkit and training resources you can download.
- NIST provides a list of free and low-cost trainings you can use today to start your program.

This safeguard supports CIS Control 14.1

Cyber Checkup Results & Recommendations | 7

Contact Center@sao.wa.gov for more information

Will your team know what to do in the first hour of a cyberattack?

SAO's Cyber Incident Response Workshop helps your team:

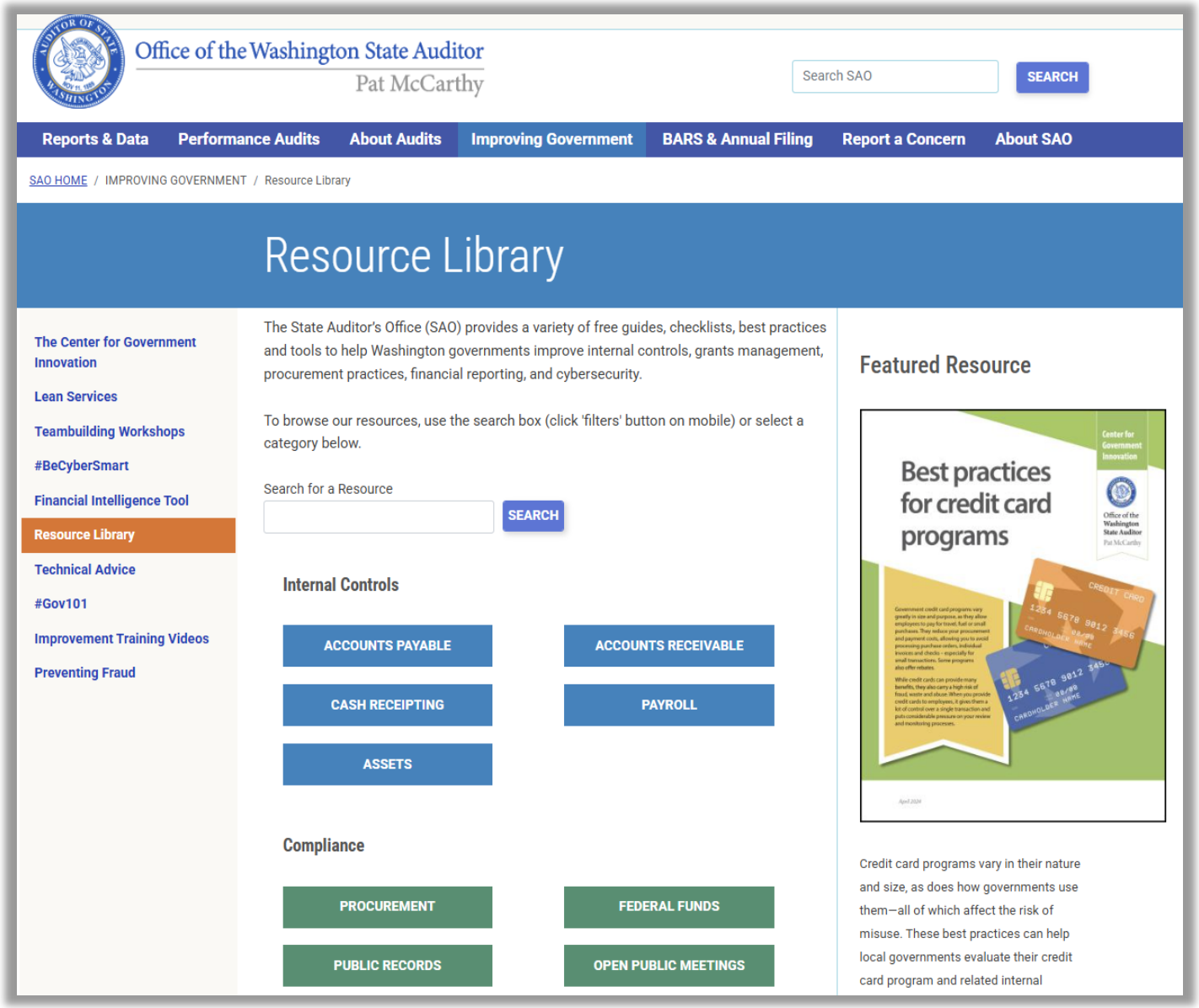
- Evaluate key decisions to customize a plan
- Develop strategies through attack scenarios
- Create a response checklist and reporting template
- Be fully prepared to handle a cyber incident



Benefits of having an incident response plan

- Make the critical decisions before an incident occurs, and without urgency
- Assign roles early so they can be learned and internalized
- Walk through example scenarios so you can be ready for the real thing
- Contact Center@sao.wa.gov for more information





Scan QR code to view the Resource Library!

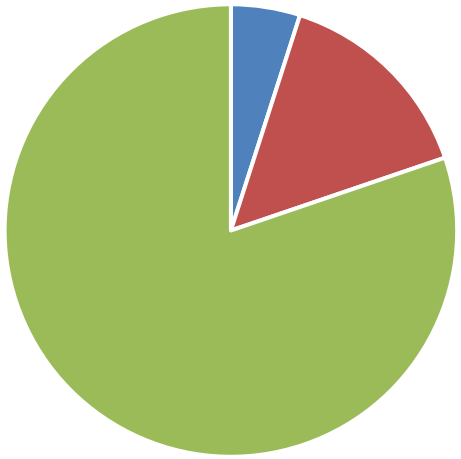
What's going on with ports

- Common audit recommendations
- Professional service procurement



Common audit recommendations

Port district audit recommendations*



Findings Management Letters Exit Items

For reports issued January 1, 2025 – May 20, 2026

9 Findings

27 Management letters

146 Exit items

Common audit recommendations

Area of Issue	Findings	Management Letters	Exit Items	Total
Fraud	1	0	0	1
Accounts Payable Disbursements	1	2	15	18
Payroll/Personnel	1	0	11	12
Federal Grants	3	0	2	5
Accounting/Financial Reporting	3	11	32	46
Purchase Cards/Credit Cards	0	1	8	9
Annual Report Filing	0	3	3	6
Cash Receipting	0	1	4	5
Financial Condition	0	1	0	1
Open Public Meetings	0	2	23	25
Procurement/Bid/Prevailing Wage	0	5	12	17
Small and Attractive Assets	0	1	4	5
Other	0	0	32	32
Total	**9**	**27**	**146**	**182**

Credit cards

Why use credit cards?

- Process efficiencies
- Vendor payment timeliness
- Immediate payment needs
- Convenience

Risks with credit cards

- Noncompliance
- Inappropriate purchases
- Fraud





Credit card risks

- Missing receipts or insufficient support
- Lack of documentation to demonstrate valid public benefit
- Lack of approval documentation
- Employee recognition spending without necessary justification or thresholds
- Non-compliance with established policy



Credit card resource

Best practices over the following areas:

- Setting up your program
- Working with credit card users
- What to do before issuing credit cards
- Processing spending activity
- Monitoring your program



Reporting personal credit card use to SAO

- Personal use is <u>never</u> allowable under state law, even if paid back
- Governments can not lend credit to individuals (Article VIII, Section VII)

** Attorney General's Letter – June 2, 2011*

RCW 43.09.185 - "Immediately report known or suspected loss of public funds or assets or other illegal activity."



Reporting personal credit card use to SAO cont.

Should I still report this to SAO if…

- It was an accident? YES
- The government was already reimbursed? YES
- The dollar amount was small? YES
- An external bad actor made the personal charge? NO

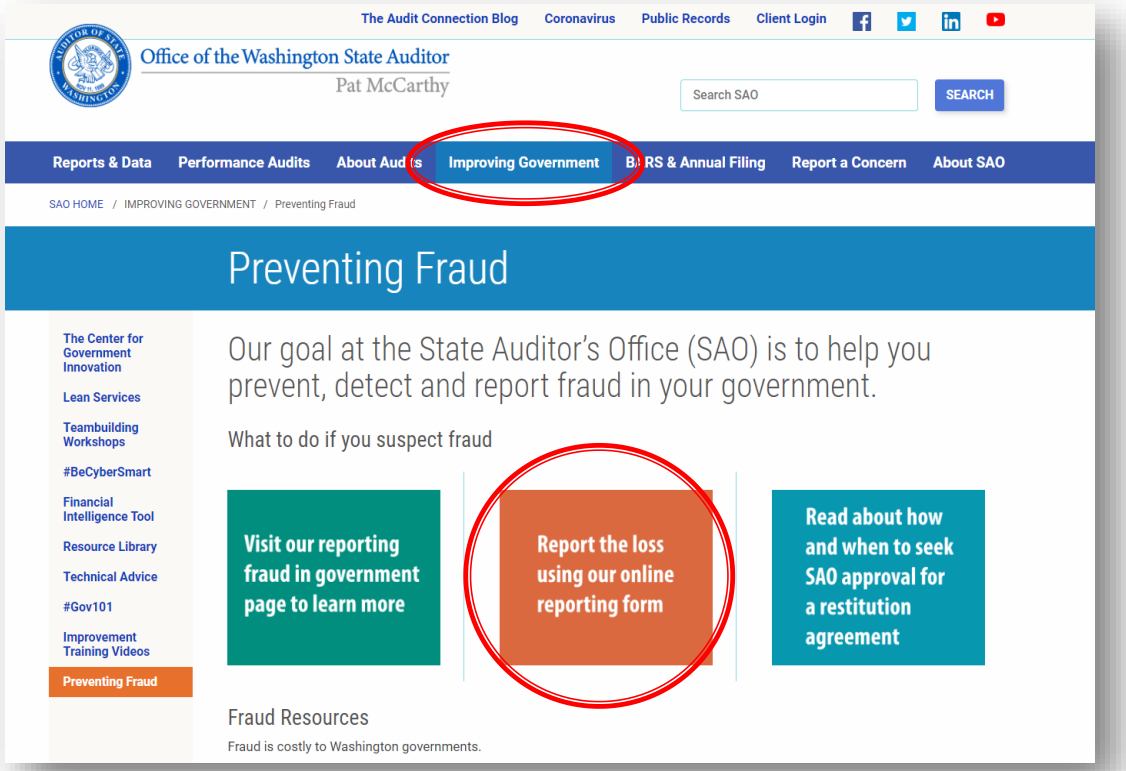
Reporting personal credit card use to SAO cont.

What does SAO do with these reports?

- Review the report and determine whether it warrants a fraud investigation
- Factors to consider
- Reporting still matters – allows auditors to assess whether there are risks to consider during the accountability audit

Reporting personal credit card use to SAO cont.

- Report any known or suspected instances of fraud or loss, or other illegal activity to SAO
- Use SAO's website and the "Report a Suspected Fraud or Loss" form
- For more information email fraud@sao.wa.gov

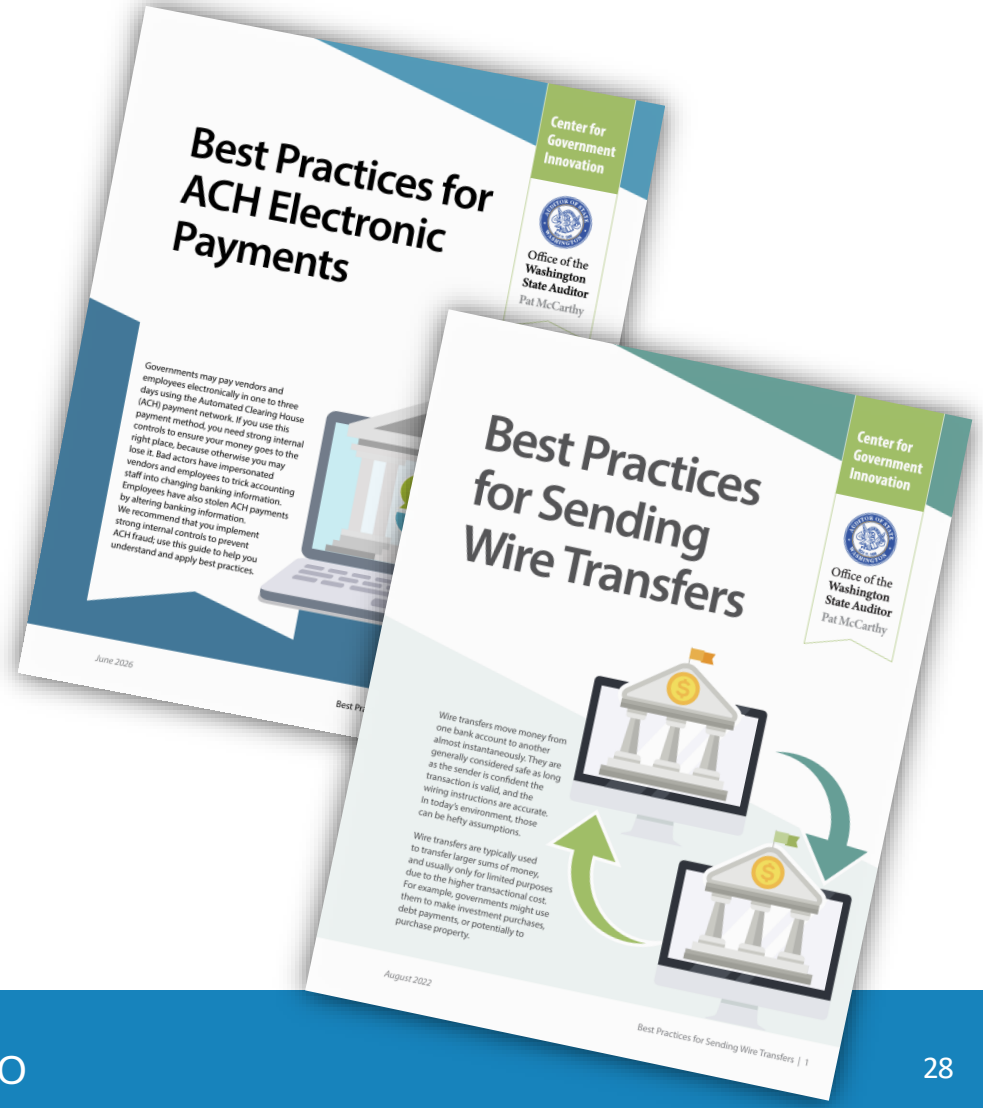


Electronic payments – change request

Loss of public funds due to remitting payment to a fraudulent bank account

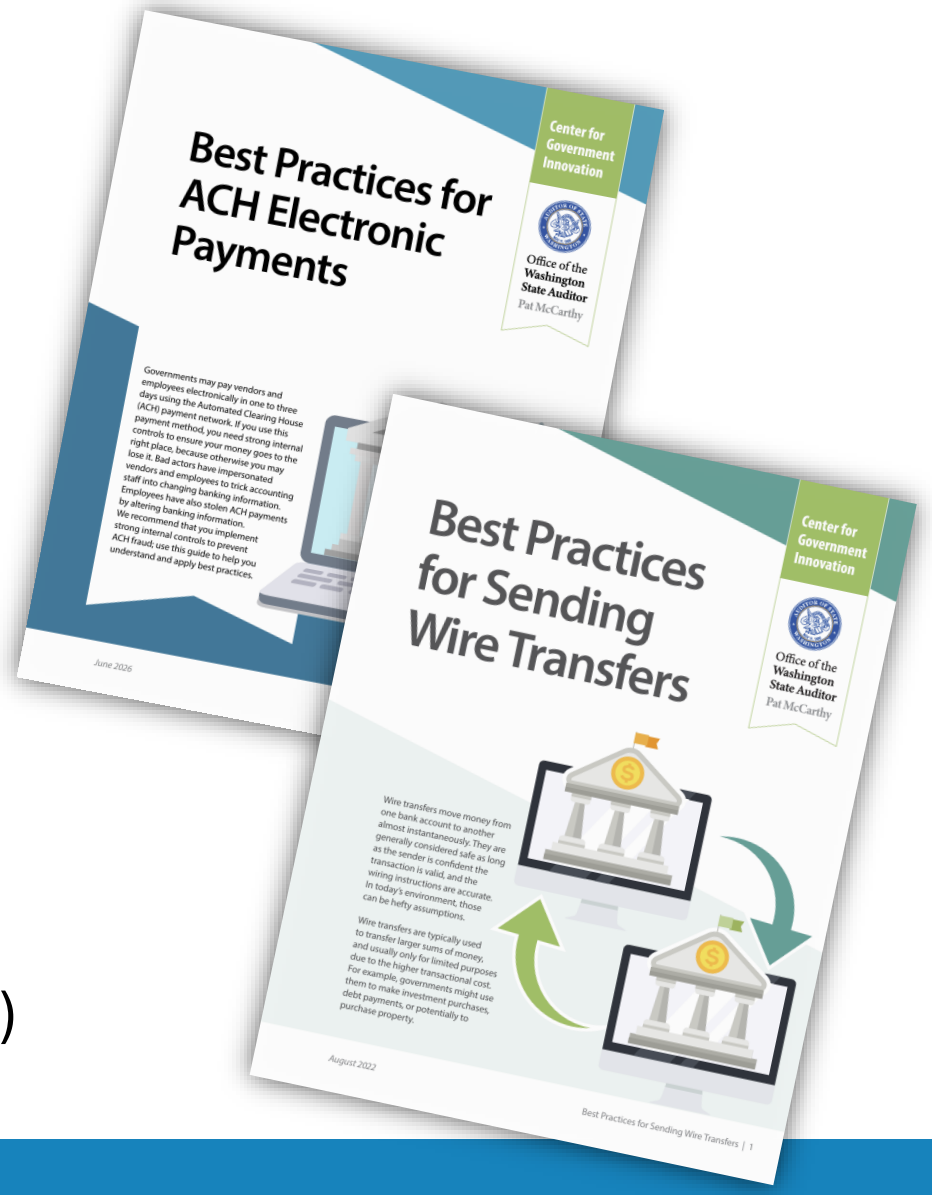
Risks identified

- Lack of policy over electronic fund transfers (EFT) that contain required elements (BARS Manual 3.8.11.30)
- Inadequate procedures to verify payment change requests
- Lack of communication of expected procedures to all staff



What can you do?

- Don’t trust email.
- Assume it’s a scam until you’re proven otherwise
- Request that employees make changes in person
- Vendors:
  - Confirm via video call you initiate
  - Provide contractors and vendors with a security key or passphrase they must provide for any contact for bank changes (do not send via email)



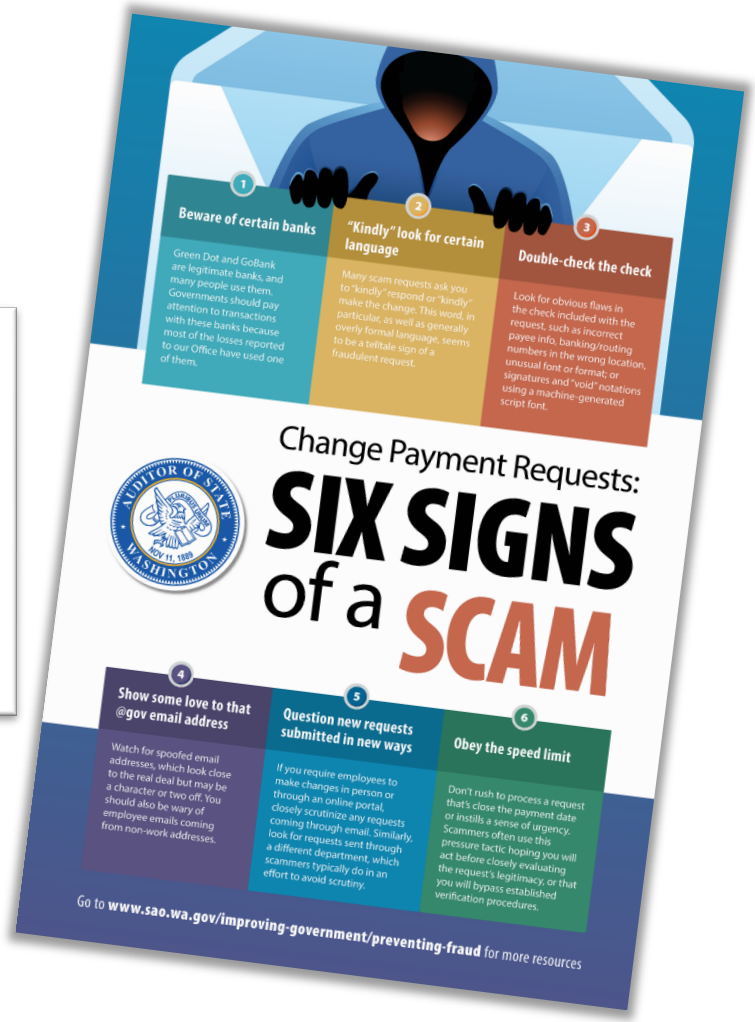
EFT resource

- **EFT policies** should include important elements that are necessary to safeguard public resources
- Policies and procedures should be in place to validate changes and authorizations to protect resources being transferred electronically
- Remember: communicate the expected procedures and policies to all staff



Six signs of a scam poster

- Print and display our “Change payment request: Six signs of a scam” poster
- Reminder of how to stay vigilant
- The six signs of a scam for payment change requests
- Perfect for your Payroll and Accounts Payable staff

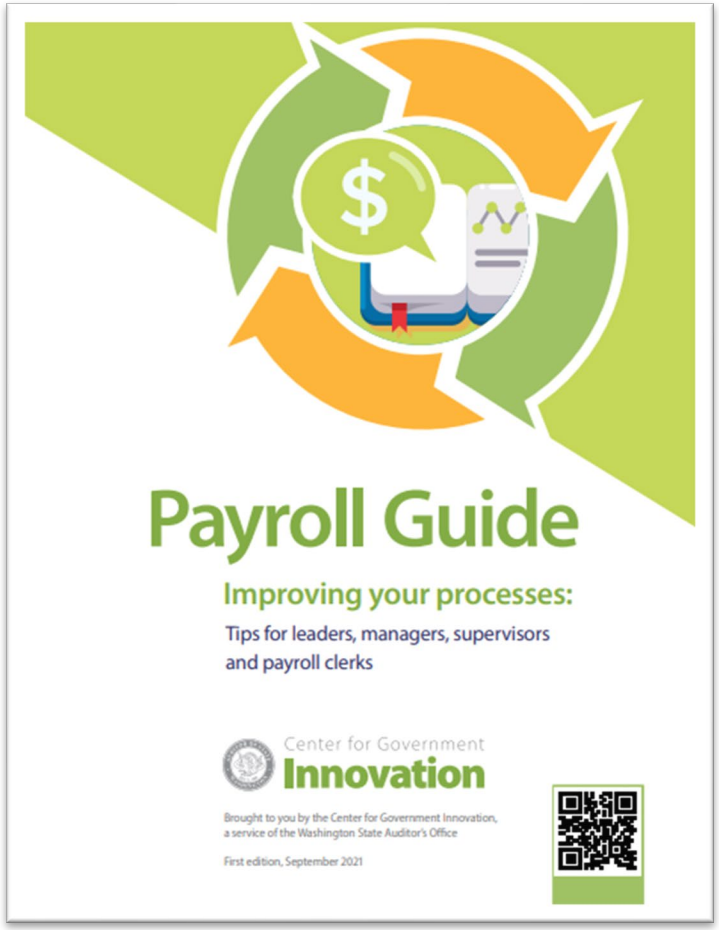


Payroll risks identified

- Pay types not supported or approved properly (retroactive pay, incentive pay)
- Incorrect leave payouts – lack of adequate documentation to support payout, noncompliance with policy
- Lack of secondary review of payroll journal entries
- Lack of policy



Tips to develop effective policies



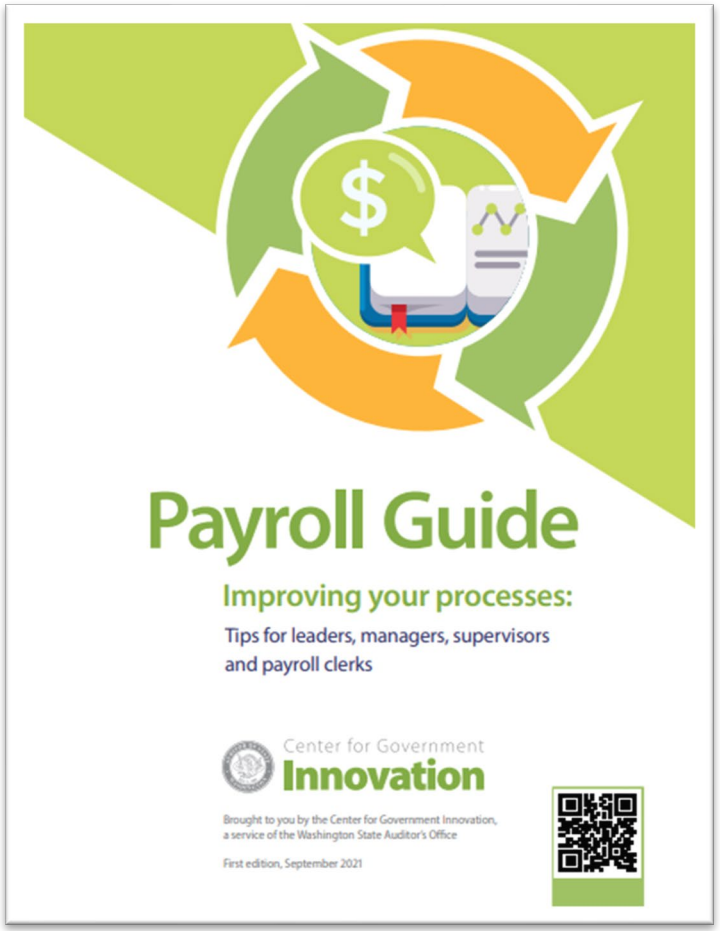
Leadership

Improve your payroll policies today!

Payroll is a significant expenditure for most governments. That's why it's important to develop guidance that covers all aspects of compensating employees, as well as specific guidance for processing payroll. While it's not possible for this resource to cover every topic you should include in your personnel or payroll policies, here are some ideas to get you started.

Salary or wage setting – Describe the documents you will maintain to support salaries, wage rates and changes to them. Designate who authorizes these key documents for the organization as a whole, for each position and for each employee.

Tips to develop effective policies



- **Non-standard compensation** – Your policy should cover all types of compensation, even those that are infrequent or only paid out in specific circumstances.
- **Timekeeping expectations** – It's important to address who is expected to record time worked, how it should be recorded, and how it will be approved. If you decide exempt employees will not submit time records, your policy should address how time off will be reported and approved for those individuals.

Architecture and Engineering

Use a competitive qualifications-based process (no dollar threshold):

- Collect statements of qualifications from firms
- Establish evaluation criteria and document the evaluation process
- Select the most qualified firm first, then negotiate price



Requirements of Washington state law

RCW 39.80.030: Each agency shall publish in advance that agency's requirement for professional services [...] by:

1. Publishing an announcement on each occasion, or

2. Announcing generally to the public it's projected requirements for any category or type of professional service



RFQ for a specific project

Procurement laws are designed to provide a fair forum for all interested bidders.

We encourage Ports to:

- Ensure your full scope of work is included in the original solicitation
- Negotiate a fair and reasonable price
- Follow your policies for necessary approvals
- Consider if modifications materially change the original scope and, therefore, need to be separately procured

RFQ for general need (on-call contracting)

- Request qualifications for a general need, by category or type of service
- Can advertise for a multi-year agreement
- Can add task/work orders as projects come up
- OR you can operate a roster, listing the qualifications you receive and revisit it when you have a project come up.



Concern – Changes in firm qualifications

- Risk with multi-year multi-project agreements:
  - Changes in firm qualifications (staff experience, licensing, ability to meet deadlines, quality and capacity)
- Considerations:
  - Consider how long the agreement should be
  - Consider a clause in procurement and agreements to ensure firm remains most qualified or cancellation if significant concerns arise



RFQ and “shall encourage”

- RCW 39.80.040 states “the agency shall encourage firms […] to submit annually a statement of qualifications.”
- “the agency shall evaluate current statements […] on file”
- Shall encourage could mean – requesting updated qualifications by email or post on your website, or a clause in the contract requesting they resubmit information annually.



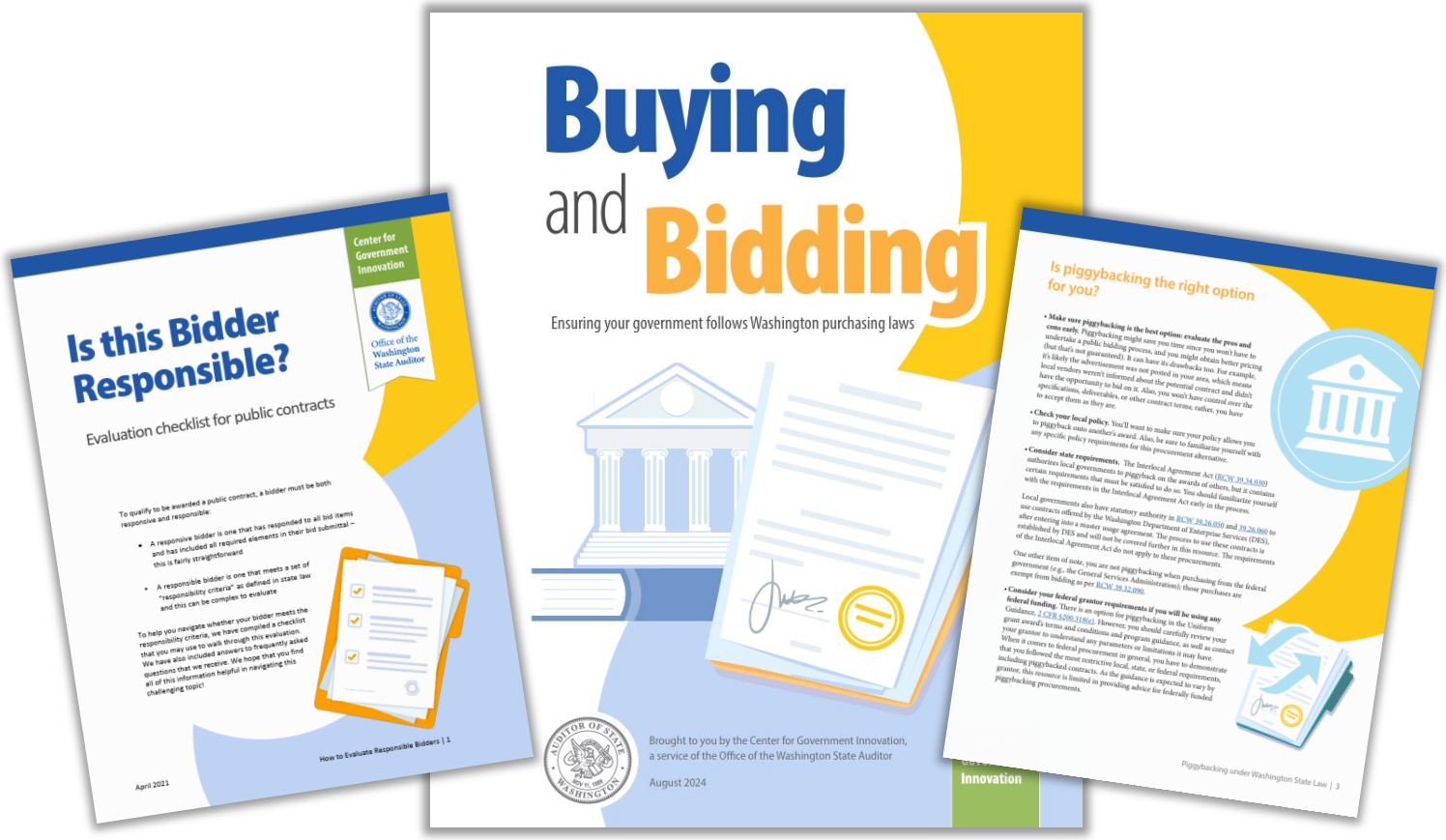
Concern – Federal grant compliance

- If using $1 of federal funds:
  - Must advertise **per project**
  - Must publish evaluation factors and their relative importance
  - Must have **written procedures** for evaluations



Buying and bidding resources

- Collection of resources aimed at compliance with buying and bidding laws
- Covers purchasing considerations using local, state and federal funding



Questions?

Contact

Josh Stohr, Team Vancouver and Port Subject Matter Expert (SME)

Joshua.Stohr@sao.wa.gov
(564) 444-6621

Deena Garza, Team Bellingham and Port Program Manager

Deena.Garza@sao.wa.gov
(360) 676-2165

sao.wa.gov

Follow us on:

