From:	Bodin, Peggy (SAO)
To:	SAO DL IT Audit Data; SAO DL IT Audit Cyber Spec; SAO DL IT Audit Systems; SAO DL IT Audit Cyber Audit; Frank, Scott (SAO); Franklin, Joseph (SAO)
Cc:	SAO DL TEAM Performance Audit; SAO DL Team Executive; SAO DL TEAM Communications; SAO DL Admin Managers; SAO DL Assistant Directors; Mann, Daniel (SAO); Munn, Aaron (SAO); Stowe, Justin (SAO)
Subject:	IT Audit Weekly Communication for December 18 , 2023
Date:	Monday, December 18, 2023 7:01:07 AM
Attachments:	image003.png image001.png

Happy Monday!

Command (Required Reading or Action Required) - lots of things to share this week

Update timesheets Daily

At the manager's meeting the requirement to update timesheets daily was reinforced. Timely updates makes a difference to the Fiscal team and it helps us flesh out time code issues more quickly. A calendar appointment to yourself or a recurring task are ways I've seen team members successfully implement this.

Use of AI Assistants in Meetings

We've noticed a few instances recently where an attendee (not SAO staff) brought an AI assistant to the meeting (the specific app was *read.ai*, but there are others). Among other things, these types of assistants create notes of the meeting, first by creating a transcript and then by summarizing that transcript. There may come a time when these apps are deemed OK to use. But for now, consistent with our moratorium on using AI, we would prefer that these apps not be used by anyone in our meetings, including the non-SAO attendees. So, if you come across one of these apps, here's what we'd like you to do:

- If you're running the meeting:
  - If you see an unknown attendee, determine if it's an AI tool. If they have brought an AI attendee, tell them we don't currently allow these tools so please turn it off.
  - If they refuse, politely tell them we'll need to adjourn and consult with management.
- If you're attending someone else's meeting:
  - Use your best judgment on whether to 1) ask them to turn it off, 2) decline the meeting, or 3) go forward with attending the meeting.

Finally, please alert your manager or principal if you encounter these situations.

Linked In (also on the Hub)

All SAO employees are getting a LinkedIn subscription for 2024 to support upcoming required training. Each of you should have received an email to activate your account. Please make sure to do the activation. If you didn't receive the email or are having trouble initiating the subscription, please contact SAOTraining@sao.wa.gov for assistance. Please note, if you've been using a library version of LinkedIn, you will still need to have a work version. They are different.

Teams Chats

Quick reminder of Pat's communication to staff (abbreviated – please make sure you read the full email):

> **The public needs to be able to learn why government does what it does**, no matter what form that information takes. If that explanatory information exists only in a Teams Chat that disappears after seven days, we aren't meeting our public duty. Teams Chat helps us work efficiently – but taking care with how you use it will help you avoid burden when managing records.
>
> Teams Chat is only for transitory communication. **Transitory communications are disclosable in response to a public records request.**

SAOShare

Each state and local government has at least one and in many cases, two or three SAOShare sites. When you are asking for information from your audit client, particularly confidential data, please make sure to specify which SAOShare site they should post the data to. This will help avoid frustrations around accessing the data you requested. AND, it will minimize unnecessary sharing of confidential information. Thank you!

Information Highway (optional reading)

Tips, Tricks and Training

NSAA-IT

- The NSAA-IT training committee is working to identify training topics for the conference next September. If you have a presentation you'd like to give OR a presentation you'd like to see included in the conference, please send the **TOPIC** to me **by 12/31/23.** I will submit the topics to the training committee. NSAA-IT is being held in Pennsylvania September 24 – 27th. Thank you!

Reading – I liked this ISACA article -

Lifelong Learning: An Essential Attitude for Career and Life Success (ISACA

Journal Volume 6 – 2023)

- "Forbes Enterprise Tech contributor, Bernard Marr cited a statistic from Dell indicated that by 2030 85% of us who are in work will be doing jobs that don't exist yet".
- "An attitude of lifelong learning is one that extends beyond being prepared for employer demands. It permeates every aspect of living – from work to leisure activities to personal enrichment."
- "There are two distinct types of learners (with distinct motivations)... those who have a natural love for learning and intellectual fulfillment and those who have a highly specific goal in mind of getting a better job or higher wages"
- "Rather than chasing after- or being chased by – the next indispensable skill, lifelong learners recognize they have the capacity to draw on their collection of character traits and habits that are adaptable to various situations…"
- "Lifelong learners are prepared to adjust and be ready for the workplace challenges they face"

Systems Audit News (Thanks, Karen!)

Payroll Master File Risks – 12/16/2023

[Since we are talking about payroll risks now is a great plug to remind everyone to ensure your information is correct in the HR Home (wa.gov) app so your tax forms make it to the right location.]

Unauthorized changes to the payroll master file present key risks during the payroll cycle. Management needs to ensure that access to the payroll master file is restricted to appropriate personnel. Too many rights to the wrong individuals increases the risk of fraudulent activities.

Auditors should ensure the logical access setup is appropriately controlled. What risks could be increased if agencies do not have adequate least privilege controls over payroll master files?

- Adding in false new hires (i.e., ghost employees).
- Changing contact/deposit information for *separated* employees rather than remove them
- Increase appointed salary/job classification
- Eliminate or reduce required employee contributions/increase employers contributions
- Unit of pay. Users may create weekly payroll for some users and semi-monthly for others. The calculation of pay and reductions and the IRS limits calculate differently based on how many pay cycles you receive a year.
- Changing/adding inaccurate bank account information to existing employees. Because

a system can also produce manual checks when needed, if certain employees prefer manual checks this opens up the opportunity for the payroll division to create both a manual check and a direct deposit elsewhere.

What are some controls agencies should consider?

- Edit checks or reconciliation between HR Active hiring list to Payroll's Profile list.
- Edit checks or reconciliation between network users and payroll list. It's assumed that all employees get access to the network for one reason or another. And if the agency has just one major program used, there could be a reconciliation between licensed users and payroll.
- Having workflows in the systems that prevents a person from making edits to their own profile.
- Having granular rights locked down to the action item. i.e., the person initiating a new hire cannot perform any additional information requiring another personnel to interact with the paperwork/information needed to complete the process.
- Locking down read-only and edit rights to selected fields such as Social Security Numbers.
- Edit checks or reconcile between employee contributions withheld to accounts payables**.**
- **Edit checks or reconciliation between the payroll submodule and the general ledger.**
- Robust audit trails that track changes down to the field levels.
- Locking down direct deposit interfacing/text files to responsible personnel.
- Having a dedicated communication between agency and bank when transferring bank account numbers.

-

News Around the State, the Nation, and the World

- Need a state AI roadmap? NASCIO has a guide for that | StateScoop
- Cyberattack on Irish Utility Cuts Off Water Supply for Two Days - SecurityWeek

The Technology Service Board approved 6 new OCIO policies for Washington State Agencies

- IT Security Audit and Accountability Policy
- IT Disaster Recovery Planning Policy
- IT Security and Privacy Awareness Training Policy
- Physical and Environmental Protection Policy
- Security Assessment and Authorization
- Remote Access Standard

Key Links

- Stakeholder meeting links including agendas, notes and status updates are here

- Complete notes from ITLT meetings can be found here.
- ITLT weekly communications can be found here.

Social Networking

Shout Outs

Congratulations to Jamie, Steven, Jessica, Lulu, Jeff and Joe- they completed the second State Cyber audit of the biennium! The exit conference took place with the volunteering state agency on Friday December the 8. Two Deputy Directors in addition to several other senior executives attended the exit and expressed gratitude for the work the team completed. It's always great to see an exit conference on cybersecurity (late Friday) so well attended.

Peg Bodin, CISA
Assistant Director of IT Audit, Office of the Washington State Auditor
(564) 999-0965 | www.sao.wa.gov
SAO has some new phone numbers. I can now be reached at (564) 999-0965.