Office of the Washington State Auditor

Pat McCarthy

Whistleblower Investigation Report

Department of Social and Health Services

Published April 13, 2020

Report No. 1026074

Office of the Washington State Auditor
Pat McCarthy

April 13, 2020

Cheryl Strange, Secretary
Department of Social and Health Services

Report on Whistleblower Investigation

Attached is the official report on Whistleblower Case No. 19-025 at the Department of Social and Health Services.

The State Auditor's Office received an assertion of improper governmental activity at the Agency. This assertion was submitted to us under the provisions of Chapter 42.40 of the Revised Code of Washington, the Whistleblower Act. We have investigated the assertion independently and objectively through interviews and by reviewing relevant documents. This report contains the results of our investigation.

If you are a member of the media and have questions about this report, please contact Director of Communications Kathleen Cooper at (564) 999-0800. Otherwise, please contact Assistant Director of State Audit Troy Niemeyer at (564) 999-0917.

Sincerely,

Pat McCarthy

State Auditor

Olympia, WA

cc: Governor Jay Inslee
Andrew Colvin, Discovery & Ethics Administrator
Kate Reynolds, Executive Director, Executive Ethics Board
Cheri Elliott, Investigator

Assertion and Results

Our Office received a complaint asserting a Department of Social and Health Services (Department) employee (subject) failed to manage a contract with the Washington Association of Prosecuting Attorneys Support Enforcement Program (WAPA-SEP) when he did not address IT security issues.

We found reasonable cause to believe an improper governmental action occurred.

Background

For decades, the Department's Division of Child Support (DCS) has worked with WAPA-SEP to provide IT hardware, software, and technical support to county prosecuting attorneys. Before the contract in question, which lasted from July 1, 2018, through June 30, 2019, one DCS employee worked exclusively for WAPA-SEP, in addition to WAPA-SEP employees who provided the technical support. During this contract, DCS began transitioning to the role of sole technical support to the prosecuting attorneys' offices involved with child support cases.

Between March 2017 and April 2019, our Office received 12 complaints related to the working relationship between DCS and WAPA-SEP. On June 27, 2018, we sent a letter to the Department Secretary informing her of the numerous complaints and the specific issues brought forward. In March and April 2019, we received the complaints surrounding this investigation — the third investigation our Office opened concerning DCS and WAPA-SEP.

About the Investigation

We reviewed thousands of emails and conducted interviews. Countless emails underscored the frustration regarding DCS's inability to get needed passwords from WAPA-SEP employees, to make improvements to IT support services for the prosecuting attorneys' offices and to access state equipment.

To determine how best to transition without disrupting business, a committee consisting of prosecutors, DCS staff and WAPA-SEP staff was convened. Throughout this process, emails show both sides questioned the technical abilities of the other. According to the subject, a major problem with the transition was the fact that the prosecutors' offices used two platforms that DCS did not use. The subject's emails showed his opinion, shared by a former DCS IT employee, that DCS staff did not have the expertise in either platform. As shown in emails, not all DCS staff agreed with that conclusion. The subject said that the decision was made to transition all the prosecutors' offices to the Windows operating system environment, the platform DCS does have expertise in, and to move the offices from the Groupwise email system to each county's email system. During the email transition, WAPA-SEP retained control over the Groupwise system.

According to the complaints, the subject was aware and did nothing to correct the following:

- Some prosecutors' office workstations and servers were out of compliance with IRS security regulations and Department security policies, both referenced in the contract. Access to DCS systems was open to untrained, non-DCS staff.
- WAPA-SEP allowed a subcontractor remote access to servers without a VPN, and without a security scan of the servers she accessed or of the personal computer she used.
- WAPA/SEP employees worked from home using state equipment, including a printer, without an inspection of workspaces.
- WAPA-SEP did not allow DCS employees access to state equipment.

Regarding the topics as outlined above:

Equipment not meeting IRS and Department security requirements, and untrained and non-DCS staff having system access

The subject agreed that systems were open to non-DCS staff, but did not agree entirely that these people were untrained. He said that some have administrative rights, which is not ideal, but rolling out the change to Windows will help close that up. He did not think that their access was a violation of IRS regulations. A witness did not agree with the statement that untrained staff were accessing the equipment, stating that the prosecuting attorney offices and WAPA-SEP ensure that employees accessing the equipment are trained properly.

We found no evidence that non-DCS staff were untrained.

Witnesses said that WAPA-SEP has not kept its systems up-to-date and because of that, they continually had problems providing support, which the subject failed to address. A witness said that the subject used the excuse that DCS cannot replace all of the counties' systems, which the witness said was true, but there were things that could have been done and the subject would not do them. A former DCS IT employee on more than one occasion stated in emails that DCS needed to get the former WAPA-SEP director out of IT and that until that occurred DCS would not be able to properly support the prosecutors' offices. The subject said that he tried to get issues taken care of but under the contract, the responsibilities were WAPA-SEP's and he could do only so much on his end.

A witness said that access to the systems by WAPA-SEP, prosecutors' offices and the subcontractor who worked out of country was because only one user ID was created by the DCS employee who worked exclusively for WAPA-SEP, referenced above, and used by many people. This was confirmed in a previous investigation, when our Office attempted to identify when the DCS/WAPA-SEP employee was working but could not do so because multiple people were using the same user ID. The witness said that rectifying the issue was as simple as shutting down that user ID and creating individual ones and granting access to systems as needed. However, according

to the witness, the subject would not allow DCS staff to do this. As stated above, the subject thought WAPA-SEP was responsible for addressing this issue. However, witnesses confirmed that the security of WAPA-SEP servers was the responsibility of DCS.

We spoke with a DES contracts employee who said that a contract with an entity does not relieve the agency from its responsibility to protect data accessible to the entity.

The Office of the Chief Information Officer (OCIO) State IT Security Policy 141.10.1.5(5) requires contractor's compliance with OCIO IT security standards relative to the services provided when (a) the scope of work affects a state IT resource or asset, or (b) the agency contracts for IT resources or services with an entity not subject to the OCIO security standards.

We disagree with the subject's assertion that the security of the servers are the sole responsibility of WAPA-SEP. We determined the subject failed to ensure WAPA-SEP complied with state IT security policies.

Remote system access by WAPA subcontractor without VPN and without security scans conducted

According to the subject and emails, it was true that a WAPA subcontractor was accessing the systems remotely without using a VPN, and that no security scans were conducted on the servers she used or her personal computer.

The subject said this was not the most secure access method, but the subcontractor was under contract with WAPA-SEP, not DCS. He said that according to the contract, WAPA-SEP was responsible for ensuring its contractors followed IRS regulations. He said the contractor could not access DCS servers, just the one WAPA-SEP server that housed Groupwise and 12 counties' file systems. He said the contractor did not have a user ID to access the DCS system. He said when DCS thought it was going to take over Groupwise, DCS planned to create a VPN for the subcontractor, but WAPA-SEP ended up using a different subcontractor and DCS did not take over Groupwise. One witness agreed with the subject, stating that the subcontractor could not access the DCS system because the subcontractor lacked a user ID specific to the system.

Other witnesses said the subcontractor did have access to the DCS system through WAPA-SEP because she was using the one user ID referenced above. In addition, witnesses did not agree with the subject's statement that the subcontractor could access only one of the servers. Witnesses said that two servers stored emails and a separate server stored case files for the 12 counties.

One witness stressed that the subcontractor did not appear to have done anything suspect, but that the lack of proper security checks made the system vulnerable.

According to the contract between DCS and WAPA-SEP, the contractor and subcontractors can access the DCS system using only Department hardware and software. The contract also requires all user accounts to be unique and logon IDs and only the assigned person know passwords, and

that it must always be possible to determine which employee accessed the system based solely on the logon ID.

A witness said that the subcontractor had unauthorized access to the state government network (SGN) and logged into state-tagged equipment, which was contrary to how things were supposed to be done.

Witnesses overwhelmingly agreed that DCS is responsible for the security of the state-tagged equipment.

We determined, based on OCIO policy, that the subject violated state IT security policies when he did not correct the issue of people sharing the same username and password, and allowed the subcontractor to connect without a VPN.

Use of state equipment at home without workspace inspections

It was asserted that WAPA-SEP employees were accessing DCS systems, on state-tagged equipment, from home without a workspace inspection. Also, that at least one employee had a state-tagged printer. Witnesses said that no IRS documents can be printed at a home workstation and there was no reason for an employee to have a printer at their home. The subject said he was not aware of someone having a printer at their home, but if there was a business need, it was up to WAPA-SEP to ensure the user complied with IRS regulations. The subject said the WAPA-SEP staff who train the prosecuting attorneys' office staff must be able to access the DCS system to conduct the training.

DCS has an inspection team that inspects the workspaces for its teleworkers to ensure they align with policies. We asked the inspection team manager if the WAPA-SEP employee telework spaces should be inspected. The division director's executive assistant responded that the team does internal site inspections for their staff primarily based on the systems accessed, but do not necessarily conduct the inspections just because DCS equipment is used in the home. In further communications with the team manager, we were told that DCS is currently scheduling an inspection of the current WAPA-SEP trainer's telework space. The team manager said that as far as he knew none of the past trainers teleworking offices had been inspected by his team. However, the current trainer said that when she first started working for WAPA-SEP in 2015, her home office was inspected by the DCS/WAPA-SEP employee, and more recently by the person now holding the WAPA-SEP director position, although she cannot recall if that was while he was still employed at DCS.

We found that trainer telework spaces were inspected in the past and that DCS was currently scheduling an inspection of the sole remaining trainer's telework space.

WAPA-SEP not allowing DCS employees access to state equipment

Regarding physical access of equipment, the subject acknowledged that there were issues accessing the servers that were in the WAPA-SEP office buildings. He said that on one particular occasion, the former director made DCS staff wait for a Pierce County employee, formerly employed at WAPA-SEP, to come down to Olympia before she allowed DCS staff access. The commute took some time and caused a delay in getting the issues corrected for the counties. The subject said that contractually WAPA-SEP must allow access to the equipment within 24 hours, and he does not think that anyone ever waited more than that. He said that things became so bad between DCS IT staff and WAPA-SEP staff that he interjected himself as the go-between when DCS staff needed access to WAPA-SEP equipment.

Witnesses thought that because DCS purchases the equipment, it belonged to the state and should be accessible to DCS staff at all times. According to a witness, having the subject as an intermediary did not go well with the employees who were responding to helpdesk tickets submitted by the counties — this approach just slowed everything down.

We found no evidence to support the assertion that WAPA-SEP did not allow DCS employees access to state equipment within the required 24-hour period.

Conclusion

Although the subject opined that WAPA-SEP was responsible for ensuring it complied with the contract, the state's Office of the Chief Information Officer has a policy (OCIO 141.10) that places the responsibility of protecting state assets in the hands of the state agency:

> **OCIO Policy 141.10: Securing Information Technology Assets**
>
> IT security planning is primarily a risk management issue. Therefore, the OCIO requires agencies to follow the IT Security policy and standards to mitigate security risks in a shared and trusted environment. Agencies will:
>
> (1) Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment.
> (2) Ensure secure interactions between and among business partners, external parties, and that state agencies utilize a common authentication process, security architecture, and point of entry.
> (3) Close unauthorized pathways into state networks and to the state's data.
> (4) Prevent misuse of, damage to, or loss of IT hardware and software facilities.
> (5) Ensure employee accountability for protection of IT assets.
> (6) Ensure and oversee compliance with these IT security standards, including the annual verification of security compliance from the agency heads to OCIO.

We found reasonable cause to believe an improper governmental action occurred when the subject did not follow state IT security policies. Due to a series of such violations, we determined the subject grossly mismanaged the contract between DCS and WAPA-SEP.

Department's Plan of Resolution

Thank you for the opportunity to review and respond to the State Auditor's Office (SAO) report on Whistleblower Case Number 19-025. The Department of Social and Health Services (department) appreciates the assistance of the SAO by providing the department with important facts from its investigation.

The report states the SAO found reasonable cause to believe an improper governmental action occurred when the subject did not follow state IT security policies. Due to a series of such violations, SAO determined the subject grossly mismanaged the contract between the department's Division of Child Support and the Washington Association of Prosecuting Attorneys Support Enforcement Program (WAPA-SEP). According to the report, the subject:

- *Failed to ensure WAPA-SEP complied with state IT security policies.*
- *Violated state IT security policies when he did not correct the issue of people sharing the same username and password, and allowed the subcontractor to connect without a VPN.*

The department recognizes the need for additional contract monitoring. However, we strongly disagree with SAOs statement that the subject grossly mismanaged the contract between the Division of Child Support and WAPA-SEP. The subject is not the assigned contract manager and therefore is not responsible to manage the contract.

The contract between the Division of Child Support and the Washington Association of Prosecuting Attorneys (WAPA), #1861-33116 and amendments 01-04, each identifies WAPA as the Contractor and the Division of Child Support's Government Liaison as the Contract Manager.

According to the contract, WAPA is responsible for:

- *Compliance with Applicable Law - At all times during the term of this Contract, the Contractor shall comply with all applicable federal, state, and local laws and regulations, including but not limited to nondiscrimination laws and regulations.*
- *Confidentiality - The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification, or loss. This duty requires the Contractor to employ reasonable security measures, which include restricting access to the Confidential Information by:*
    - *Allowing access only to staff that have an authorized business requirement to view the Confidential Information*

- *Physically Securing any computers, documents, or other media containing the Confidential Information,*
- *Following the requirement of the DSHS Data Security Requirements exhibit*

- *Notification of Compromise or Potential Compromise - The compromise or potential compromise of Confidential Information must be reported to the DSHS Contact designated on the Contract within one (1) business day of discover. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.*
- *Statement of Work - The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth below:*

    - *Adhere to DSHS policies and procedures regarding the use of the DSHS Systems, particularly Administrative Policy 15.15 – Use of Electronic Messaging Systems and the Internet. Contractor shall ensure that all "Project Employees" and any subcontractors are aware they are subject to these requirements.*

        - *Ensure that Project employees and any subcontractors who have access to DSHS/DCS systems have reviewed DSHS IT security policies and system policies and have implemented all necessary security measures, including but not limited to, password protections.*

    - *Adhere to IRS Data Security requirements as set forth in Exhibit C – IRS Publication 1075, Exhibit 7 and by providing the SEMS annual employee on-line certifications for database access.*

WAPA has a contractual obligation to report contract discrepancies or violations to the contract manager. Following department policies and procedures, the contract manager is responsible to ensure contractor compliance with the terms, conditions and requirements of the contract. If a discrepancy or violation occurs, the contract manager is required to take timely corrective action, and when practicable, allow the contractor an opportunity to correct the identified problem. During corrective action the contract manager may elicit the technical experience of others such as, but not limited to, the Division Director, Policy Chief or Information Technology Chief.

Plan of Resolution

The contract manager responsible for monitoring the WAPA-SEP contract is relatively new to the position. The department will provide additional training to the contract manager to ensure adequate compliance with department policy covering contract monitoring requirements. This policy requires all department staff responsible for contracts or contract monitoring complete the Basic Contracts Certification training offered by the DSHS Contracts Academy, and the Department of Enterprise Services' WA State Contract Management 101 training. In addition,

each Administration responsible for contract management is required to:

- *Conduct a risk assessment of each type of service to be contracted.*
- *Develop contract risk assessment and performance-monitoring tools to be used for individual contracts and contractors.*
- *Develop risk assessment and performance-monitoring plans for specific contracts.*
- *Monitor individual contracts.*
- *Document the results of monitoring efforts in the contract file and/or in the Agency Contracts Database (ACD) with exception of those exempted in the scope of Policy 13.11.*

The WAPA-SEP contract is subject to renegotiation, which the Department will initiate when appropriate. After terms are negotiated and finalized, the department will carefully and specifically review the Information Technology Security Policies with the contractor, ensuring the contractor is fully aware of and prepared to accept their role and responsibility in this regard. The contract manager will monitor the contract to ensure contractor compliance with the terms, conditions and requirements of the contract.

State Auditor's Office Concluding Remarks

The SAO understands that the subject was not the official contract manager during the investigative period. When the investigation began, a conversation took place between the subject and our Office during which we asked the subject whether he would be the responsible party to correct the issue if we found that WAPA-SEP's security requirements were not compliant with IRS and DSHS regulations. The subject acknowledged that he would be the responsible party in the capacity of his job duties, but not as it related to the contract.

The DES Washington Contract Manual, which is required reading for all state employees who work with state contracts, makes clear that employees need not have "contract manager" in their position title to be responsible for contract management duties.

In addition, the fact that it has a contract in place does not relieve the Department of its responsibilities to ensure compliance with state IT security policies. While the contract requires WAPA-SEP to comply with security requirements, it is the Department's responsibility to ensure that its contractor complies.

We re-affirm our finding that the subject was aware of the violations and failed to take steps to protect state data as required of his position and state cybersecurity policies.

WHISTLEBLOWER INVESTIGATION CRITERIA

We came to our determination in this investigation by evaluating the facts against the criteria below:

RCW 42.40.020(4)

> "Gross mismanagement" means the exercise of management responsibilities in a manner grossly deviating from the standard of care or competence that a reasonable person would observe in the same situation.

OCIO Policy 141.10.1.5 Compliance

> Require contractor's compliance with OCIO IT security standards relative to the services provided when:
>
> a. The scope of work affects a state IT resource or asset.
>
> b. The agency contracts for IT resources or services with an entity not subject to the OCIO IT security standards.
>
> Contractor compliance may be demonstrated by mapping comparable contractor controls to these IT security standards, and by adding supplemental controls that close gaps between the two.

OCIO Policy 141.10.5.3. External Connections

> Agencies with devices connected to the SGN must:
>
> (1) Prohibit direct public access between external networks and internal systems.
>
> (2) Connect agency networks to the SGN through a CTS-managed security layer.
>
> (3) Ensure connections between internal networks on the SGN and external networks are made through a CTS-managed security layer. The CTS-managed security layer includes, but is not limited to, firewalls, intrusion detection systems, proxy servers, security gateways, VPN and other security and monitoring systems as deemed necessary by CTS to protect the integrity of the SGN.

OCIO Policy 141.10.6.1.2 Access Security

Accounts

To ensure appropriate management of user accounts on system components agencies must:

> (3) Identify users with a unique identifier, for their individual use only, before allowing them to access components, systems, networks, or data.
>
> (4) Ensure that accounts are assigned access only to the services that they have been specifically authorized to use. . . .
>
> (12) Prohibit the use of group, shared, or generic UserIDs/passwords.