Office of the Washington State Auditor

Pat McCarthy

June 6th, 2023

City of Tenino
149 Hodgden St. S.
Tenino, WA 98589

We are pleased to confirm that the Office of the Washington State Auditor (SAO) will conduct an information technology (IT) security audit for and at the request of the City of Tenino. This letter confirms the nature and limitations of the audit, as well as responsibilities of the parties and other engagement terms.

Our responsibilities

We will perform our IT security audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain reasonable assurance that evidence is sufficient and appropriate to support the findings and conclusions.

Your responsibilities

The City of Tenino is responsible for the design, implementation and maintenance of internal controls relevant to the city's IT policies and processes.

You, or the person you assign, will provide the information we need for performing the audit. You are also responsible for the accuracy and completeness of that information. You will need to tell us about any documents, records, files or data that contains information covered by confidentiality or privacy laws (such as information regarding IT infrastructure and security of computer and telecommunications systems, HIPAA, CJIS, or Payment Card Industry (PCI) data). When information is transmitted electronically, you will need to use secure communication methods; our audit team can give you access to our secure file transfer system.

Working with subject matter experts

We will be working with subject matter experts during this audit. We are responsible for directing the scope of their work and receiving their work products. We will give you the results of their work in unaltered form to ensure clear communication, and you will have direct access to them during the audit so you can clarify audit results. Members of the audit team will participate in or be present when the subject matter experts are conducting their work and during all communications.

Audit scope, objectives and methodology

Scope

The audit will assess the extent to which the city's IT security programs, including their implementation and documentation, align with selected *Center for Internet Security (CIS) Controls* and their supporting sub-controls. This audit will not assess the city's alignment with federal or state special data-handling laws or requirements.

Objectives

To help the city protect its IT systems and secure the data it needs to operate, we will conduct a performance audit designed to identify opportunities to improve IT security. This audit will answer the following questions:

- Does the city have vulnerabilities in its IT environment that could lead to increased risk from external or internal threats?
- Do the city's IT security practices align with selected security controls?

Methodology

To answer the audit objectives, we will compare the city's IT security programs to selected leading practices and conduct limited technical testing on the city's internal network to determine alignment with specific controls.

Vulnerability Testing

To determine if the city has vulnerabilities in its IT environment we will conduct limited technical testing and analysis of select portions of the city's internal network using automated tools configured and ran by our SAO IT security specialists. Additionally, our contracted subject matter experts will be performing penetration testing. This includes identifying vulnerabilities and assessing them to determine whether they could be exploited.

Comparing the city's IT security programs to leading practices

To determine how closely the city's IT security practices align with leading practices we will review IT security policies and procedures, interview key IT staff, and collect evidence to confirm the implementation of controls through screen shots or observations of security practices and settings. We will also conduct limited technical analysis of the city's systems.

We will use selected controls from the *CIS Controls, version 8*, as our criteria to assess the city's IT security programs and to identify areas that could be improved.

Audit costs and timeline

The City of Tenino will not be charged for the work performed in this audit. In an effort to balance a high demand for these audits with our limited resources, the city will be provided an audit start date upon completion of this engagement letter. We expect the duration of this work to take approximately 9 months, subject to the timeline conditions noted. We will discuss changes to the timeline in our regular communications with you and we ask that you communicate any scheduling restrictions to our team as well.

This audit work will take place in six phases:

1. Information request: Once we receive your signed copy of this engagement letter, and as we approach the start date, we will schedule a kick-off meeting. We will introduce the audit team, and give you a list of the materials we need from you to begin our planning work, including questionnaires addressing specific areas of IT security at the City of Tenino. If necessary, we can help you decide who should fill in the questionnaires; you can also use the questionnaires to describe any requested information that is not available.

2. Audit planning and scoping: As soon as we receive the requested materials and the questionnaires, we will begin planning the audit which will include remote meetings to learn more about your government. The planning and scoping phase will be complete when we mutually finalize and sign the rules of engagement documents, which includes the timeline for vulnerability testing.

3. Vulnerability Testing: This testing is performed by SAO's security team for the purpose of identifying internal network vulnerabilities and other areas for security improvement. Testing usually begins about two weeks after the rules of engagement are signed. Testing will take place on-site or via remote means, and generally takes one to two weeks on-site or remote. Off-site analysis takes about four to eight additional weeks after the completion of core work. We expect to deliver detailed results to Jen Scharber between eight and ten weeks after the core work has been completed.

4. Controls Assessment: Control assessment work starts a couple weeks after the core work of vulnerability testing has been performed. The initial step is to perform assessment interviews regarding all in-scope controls that are being assessed. This generally takes place in one or two weeks and consists of four on-site or remote interviews, each lasting about 2 hours. Evidence is then gathered over the following six to eight. We expect to deliver detailed results to Jen Scharber between ten and twelve weeks after the interview work has been completed.

5. Penetration Testing: This testing is performed by a third-party vendor and consists of detailed internal and external testing on specific applications and systems. Testing usually begins about two weeks after the rules of engagement are signed. Testing will take place on-site or via remote means, and generally takes two to three weeks to fully complete. Off-site analysis takes about four additional weeks after the completion of on-site work. We expect to deliver detailed results to Jen Scharber between four and eight weeks after the on-site work has been completed.

6. Exit, reporting and public hearing: Once all core work is completed, we will prepare a confidential results briefing document and provide it to Jen Scharber. We will then schedule an exit conference with you to discuss the audit results. The city will also have the option to hold an Executive Session to brief those charged with governance of the audit results. If the city chooses to not hold an Executive Session to review the confidential results we will request that Jen Scharber brief the appropriate individual(s) charged with governance on the audit results (report) and confirm in writing when the briefing has been completed.

This audit is one in a series of audits that will be publicly reported to the State Joint Legislative Audit & Review Committee (JARC). The city will not be named in this report and all information shared will be aggregated and anonymized. We will inform the city when this report has been published and when the hearing will take place with JLARC.

Expected communications
During the course of the audit, we will communicate with Jen Scharber, within 24 hours of detecting a risk we, or our subject matter experts, consider critical.

During the testing phase of the audit, we will communicate weekly on the audit status, any significant changes in our planned audit scope or schedule, and preliminary results or recommendations as we develop them.

It is the responsibility of Jen Scharber to provide regular feedback on issues that might affect the audit timeline or expected resolution of critical risks. We expect Jen Scharber will also keep us informed of any other concerns or problems that come to the city's attention during the audit.

Subsequent reference, if any, to the City of Tenino's IT security audit will only refer to local government IT audits in the aggregate and will not disclose the city's name without approval by the city.

By signing and returning this letter you acknowledge that the foregoing is in accordance with your understanding. Please contact us with any questions.

We appreciate the opportunity to be of service to you and look forward to working with you and your staff.

Sincerely,

____
Erin Laska *Date*
IT Audit Cybersecurity Audit Manager
Washington State Auditor's Office

Client Response:

This letter correctly sets forth our understanding.

____
Wayne Fournier *Date*
Mayor
City of Tenino