# Cybersecurity Services Offered to Washington Governments

The State Auditor's Office continues to expand its program of work around cybersecurity and information technology systems at both state agencies and local governments. Our goal is to help diminish the likelihood government organizations, no matter how large or small, will fall prey to hacking, malware or phishing schemes. Here's a snapshot of services we offer.

## Cyber checkups

While not intended to be a replacement for a detailed audit, these checkups are designed to be a high-level assessment of a local government's cyber health to identify gaps that could leave its IT systems vulnerable to common threats. Every checkup offers ideas on how to improve. Performed by SAO's Center for Government Innovation, these checkups are built on the framework developed by the Center for Internet Security (CIS) in its Critical Security Controls. The checkups are done remotely and can be completed in less than a month, depending on a government's availability. There's no waitlist! To schedule a cyber checkup, governments should contact the Center at center@sao.wa.gov.

## Ransomware audits

These audits examine a government's resiliency to ransomware, a type of cyberattack designed to deny access to a computer system or the data it stores until the victim pays the demanded ransom. We examine five control areas that apply to distinct facets of ransomware prevention, detection and response. These audits can benefit governments large enough to employ cybersecurity staff as well as smaller governments that use contracted IT services.

## Critical infrastructure audits

These audits are designed around the special security needs of governments that provide essential services such as hospitals, power stations and water. These smaller scoped audits focus on finding "low-hanging fruit" for improvements. We look at internet-facing assets, such as public websites, to identify vulnerabilities that an attacker anywhere in the world could leverage. We also interview IT staff and assess publicly available information to identify risks including compromised email accounts and potential data breaches.

## Cybersecurity audits

Our full cybersecurity audits dig deep into IT systems used in government operations to identify weaknesses that could expose the government to a wide range of possible risks. Audit teams conduct penetration and technical tests, and interview IT staff and managers to learn about controls already in place. Auditors then propose solutions to help strengthen those systems. To learn more about the cybersecurity audits listed here, or to request one, governments should email SAOITAudit@sao.wa.gov

## How to learn more

On September 11, we published a new report that summarizes the results of FY 2023 cybersecurity audit work. You can also view a roll-up report touching on all aspects of this work on our website at sao.wa.gov.