Written Statement of Theodore J. Sayers
Director, Intelligence & Incident Response
Center for Internet Security
Meeting of the
Joint Legislative Committee on
Information Management and Technology
Oregon State Legislature
Wednesday, May 3, 2023

Co-Chair Nathanson, Co-Chair Woods, members of the Committee, thank you for inviting me today to this hearing. My name is Theodore Sayers, and I serve as the Director of Intelligence & Incident Response for the independent, nonprofit Center for Internet Security, Inc. (CIS).[1] I directly support the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS- and EI-ISAC), divisions of CIS, which serve as the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments and election offices.

I have spent the entirety of my career in service to the government, including eight years with the U.S. Department of Defense in active duty and ongoing reserve military capacities with the U.S. Navy. I truly appreciate this opportunity today to share our thoughts on the cyber threats facing critical infrastructure at the state, local, tribal, and territorial (SLTT) level and how we can improve cyber defense across the board.

I have prepared and submitted written testimony, and I respectfully request that it be submitted for the record if the Committee is doing so at this meeting.

This morning, I will briefly: (1) introduce you to CIS and the MS-ISAC; (2) discuss the scope of the threats facing SLTT governments and municipal-run critical infrastructure today; and (3) describe MS-ISAC and CIS services that the state of Oregon and its constituent local governments organizations can leverage at low or even no cost to reduce threat exposure.

(1) **About CIS**

CIS was established in 2000 as an independent nonprofit organization, with the mission to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for security hardening of commercial information technology (IT) systems at a time when there was little online security leadership. Today, CIS works with the global security community to define security best practices for use by government and private-sector entities alike. We provide cyber expertise in three main program areas: (1) the Multi-State and, more recently, the Elections Infrastructure Information Sharing and Analysis Center, the MS-ISAC and EI-ISAC respectively; (2) the CIS Benchmarks, including CIS Hardened Images; and (3) the CIS Critical Security Controls, each of which has a part to play in the topic at hand.

[1] Find out more information about the Center for Internet Security here: https://www.cisecurity.org/

MS-ISAC.[2] Founded in 2003, the MS-ISAC was designated by the U.S. Department of Homeland Security (DHS) in 2010 as the trusted resource for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments and Fusion Centers. Its membership includes all 56 states and territories, and more than 15,000 other local government entities, including cities, counties, schools, hospitals, public safety, and publicly owned utilities, such as water, electricity, and transportation, including port authorities and airports.

EI-ISAC.[3] Following the 2016 election, various local and national groups recognized the need for an ISAC devoted solely to the Nation's elections infrastructure and, in 2018, CIS created the EI-ISAC. Leveraging the experiences, resources, and relationships of the MS-ISAC, the EI-ISAC is now fully operational with all 50 states and D.C. participating, and over 3,500 total members, including the election vendor community.

The CIS Benchmarks and Hardened Images.[4] CIS is the world's largest independent producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Benchmarks (also known as "configuration guides") provide highly detailed security setting recommendations for a large number of commercial IT products, such as operating systems, databases, and networking devices. More than 200 Benchmarks have been developed and are available for free on the CIS website. The CIS Benchmarks are referenced in a number of recognized security standards and control frameworks. CIS also offers virtual machine (VM) images hardened in accordance with the CIS Benchmarks, which provide users with a secure, on-demand, and scalable computing environment.

The CIS Critical Security Controls.[5] CIS is the home of the CIS Critical Security Controls, the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene and defendable network environments. They are developed by an international community of volunteer experts and are available at no cost to the public. The CIS Critical Security Controls protect against approximately 86% of all attack vectors identified in the MITRE ATT&CK framework.[6]

For your information, the State of Oregon is familiar with the CIS Critical Security Controls and has adopted them previously in, for example, the 2020 Secretary of State, Oregon Audits Division Cybersecurity Controls Audit of the Oregon State Police.[7]

---

[2] Find out more information about the MS-ISAC here: https://www.cisecurity.org/ms-isac/
[3] Find out more information about the EI-ISAC here: https://www.cisecurity.org/ei-isac/
[4] Find out more information about the CIS Benchmarks and Hardened Images here: https://www.cisecurity.org/cis-benchmarks/ and https://www.cisecurity.org/cis-hardened-images
[5] Find out more information about the CIS Controls and download them for free here: https://www.cisecurity.org/critical-controls.cfm
[6] CIS's Community Defense Model: https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0
[7] https://sos.oregon.gov/audits/Documents/2020-17.pdft

(2) Cyber threats facing local governments and municipal-run critical infrastructure today

The nation's SLTT governments are rich targets for cyber threat actors (CTAs). SLTT data is valuable: it contains personally identifiable information (PII), private health information (PHI), and data on finances, contracts, future business, and potentially much more sensitive operational data. SLTTs are also resource poor: they tend to lack the money, people, training, and experience to adequately protect their networks and data from rapidly evolving cyber threats. The speed at which CTAs change their tactics, coupled with the near constant turnover of security technology, can require fully staffed and dedicated teams of cybersecurity professionals just to keep from falling behind.

Through the MS-ISAC, CIS has monitored cyber threats against SLTTs and critical infrastructure for the last 20 years. Some of the most significant and impactful threats these communities have faced in recent years include the following:

1. **Ransomware**: Ransomware is a form of malware programmed to encrypt or lock files, rendering systems unusable. CTAs demand a ransom in exchange for the key to decrypt or unlock these files, often threatening to post stolen data online if not paid. This second threat is known as double extortion.

   Ransomware attacks have become increasingly common against SLTT governments. These attacks can result in critical data becoming inaccessible until a ransom is paid. Such incidents range from simple automated attacks against one device to more complex operations involving ransomware that moves laterally across entire business networks. The current threat landscape includes many complex Ransomware-as-a-Service (RaaS) operations, where cybercriminal organizations hire affiliates to gain initial access, exfiltrate data, deploy the ransomware, and then launder the stolen material and revenue. These criminal networks can even mirror legitimate business structures. Ransomware has real-world operational impacts when deployed against SLTTs, including missed school days, canceled exams, loss of legal, financial, and medical records, as well as the shutdown of safety control systems for water sanitation or other life impacting operations.

2. **Social Engineering attacks**: Social engineering attacks often seen used against SLTTs include two email-based attacks, phishing and Business Email Compromise (BEC), and a text message attack known as smishing.

   Phishing is an attack conducted over email that seeks to collect sensitive information from targets or trick users into downloading a malicious payload. Smishing uses text message technology for the same purposes. While phishing has long been the principal initial infection vector for many attacks against SLTTs, smishing is growing in prevalence, specifically related to the election community and taxation fraud. Both phishing and smishing can result in malware infections and the theft of sensitive data, including credentials, which can then be used to access restricted networks, systems, and applications for further malicious purposes.

BEC is an email attack unique from phishing wherein CTAs attempt to deceive victims into sending money, personally identifiable information (PII), or material goods, or modifying direct deposit information. The emails often originate from compromised or fraudulent email accounts and if fulfilled may result in significant financial loss or data exposure. BEC tends to use social engineering attacks that pressure victims into believing an authority figure is making the request.

3. **Unsecured or unpatched remote services**: The increased adoption of public facing and remote access technology in the SLTT community to support end user experience and efficiency as well as remote employees increases risk of exposure.

   CTAs specifically seek out and identify unpatched, misconfigured, or vulnerable versions of public facing and remote access software to gain unauthorized or privileged access to networks. Leveraging these techniques enables CTAs to appear like legitimate users, making them difficult to detect without specific expertise in identifying anomalous behavior, which requires a robust normalcy baseline for comparison.

4. **Supply chain or service provider attacks**: SLTT governments rely on third-party software and providers to perform essential functions. Unfortunately, while essential for business, third-party software and providers may unwittingly introduce weaknesses into SLTT environments that can be exploited by attackers, and to which the SLTT has no control or ability to mitigate, if they can even gain awareness of the risk. For example, the SolarWinds supply chain code compromise attack 2020 impacted SLTT governments across the US, as well as thousands of commercial organizations globally. More recently, the 3CX compromise is estimated to have impacted more than 600,000 organizations globally, including SLTTs.

Much of the nation's critical infrastructure is owned, operated, and managed at the state and local level. This infrastructure includes electrical generation and power grids, pipelines, nuclear power, clean water and wastewater treatment, air traffic control, seaports, airports, railways, emergency services, and public health facilities, among many others. The operational technology (OT) that powers these critical systems has rapidly become a target of interest for CTAs, whereby more recently, adjacent IT networks are becoming intriguing vectors for CTAs to impact OT systems. We must accept that IT and OT have converged. There is no longer enough separation between the two domains to rely on the concept of an "air gap" to protect critical infrastructure and OT systems from cyber threats.

Over the past few years, attacks on critical infrastructure have become major news stories largely due to their widespread impact. Two of the most well-known examples are the cyber-attacks against Colonial Pipeline, a privately-owned company based out of Houston, Texas that operates the single largest pipeline for refined oil in the U.S., and JBS Foods, the world's largest meat processing company. Presently, exceptionally few critical infrastructure attacks are sophisticated enough to directly impact OT systems, especially those conducted by financially driven CTAs. The bad news is that they don't have to be to have a significant impact and potentially

compromise the integrity of the industrial environment.

In both the Colonial Pipeline and JBS Foods attacks, as well as the attack on Honda in 2020 and Norsk Hydro in 2019, the systems affected were not control systems, but standard computer systems used for business operations. Likewise, all of these attacks were conducted by criminal CTAs interested in a payday. These attacks involved ransomware, which is the most common and impactful cyber threat affecting SLTTs today. While none of these entities were SLTT owned and operated, the second and third order effects of these attacks significantly impacted SLTT communities. For example, the Colonial Pipeline attack affected fuel supplies to municipal airports and transportation.

Despite some groups claiming that they will not target critical infrastructure, these networks continue to be attractive targets for cyber criminals and under many of the ransomware-as-a-service models, affiliates may target critical infrastructure, despite conflicting intentions of some ransomware developers. This is of specific concern to defenders of critical infrastructure at the municipal level for a several reasons: (1) true air-gapping of critical infrastructure, the process of keeping systems wholly disconnected from the Internet, is not practical or surefire; (2) a ransomware infection will deny access to systems that could be essential in monitoring, administering, and controlling OT systems; (3) the criticality of these systems puts pressure on organizations to pay massive ransoms; and (4) due to the evolution of the ransomware model, paying a ransom does not necessarily result in a full departure of criminal actors from the victim environment. With regard to ransomware, we can expect to see more critical infrastructure targeted as the goal of the actors is a quick payday, and few organizations have the uptime requirements as those in this sector.

Thinking beyond ransomware, state affiliated actors and cyber criminals may have specific interest in critical infrastructure and OT systems for a variety of reasons. Those can include espionage, destruction, delay, and even influence operations. There is a clear spectrum of state responsibility, wherein a state can directly support cyber operations on one end or tacitly encourage criminal activity by actively ignoring it on the other. No matter the reason, it is important for us to recognize that CTAs will increasingly target networks and systems of interest to the US, especially those deemed as critical infrastructure, to gain economic or financial, political, social, and military advantage. Since critical infrastructure is increasingly becoming connected to or reliant upon internet-connected devices, we should expect to see an increase in successful attacks until we adapt a true culture of cybersecurity.

(3) Low- and no-cost cybersecurity services available to Oregon local government

To protect against the threats described in the previous section, SLTT governments must take deliberate steps to implement strong cybersecurity measures. A rising tide lifts all boats and the fastest way to raise the tide for the entire state of Oregon is to leverage the community and resources already available for SLTTs through the MS-ISAC. Community and partnerships are the single most important factors for low-resourced communities to gain capability quickly.

Through our Cooperative Agreement with the federal government, managed in partnership with DHS's Cybersecurity and Infrastructure Security Agency (CISA), the MS-ISAC is able to

provide access to no-cost cybersecurity solutions for SLTT governments. Our 24x7x365 Security Operations Center (SOC) provides real-time monitoring and analysis for SLTT governments only. Our Cyber Threat Intelligence (CTI) team monitors CTA activity and the changes to their tactics, providing threat intelligence feeds and products to SLTTs that can be ingested into defenses for proactive protection of cyber threats. Our Cyber Incident Response Team (CIRT) responds directly to active intrusions affecting SLTTs, including full forensic investigations and associated recommendations. Our Vulnerability Management Program (VMP) aims to identify vulnerabilities before the adversary does and our Cyber Threat Liaison (CTL) team directly interfaces with operational CISA teams, bringing an SLTT perspective to federal response efforts and catering federal guidance for SLTTs.

Our Malicious Domain Blocking and Reporting (MDBR) service is a cloud-based solution that prevents computers from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability is helpful in blocking many malware infections just by preventing the initial outreach to a malware delivery domain, including those used to deploy ransomware. It is easy to configure, taking only fifteen minutes to set up.

The intent of the federal government was that the basic products and services funded by the CA would spur demand from SLTTs for extended services that would benefit from the economies of scale and the MS-ISAC's expertise in cybersecurity analysis, threat intelligence, operational lessons learned, and community best practices. This strategy, namely that the federal government provides the equivalent of basic cable through the MS-ISAC and SLTTs then invest in the premium channels through addition services with the assistance of CIS, has paid substantial dividends, with SLTTs continuing to make substantial investments beyond those from the federal government.

In response to feedback from SLTT members, CIS has expanded our free MDBR service into a paid-for service called MDBR+, granting more granular control to SLTTs that have more stringent requirements in web content filtering and custom allow and/or block lists, such as K-12 schools and public higher education.

CIS offers a number of additional services at low or no cost to SLTTs, including our Albert Intrusion Detection System (IDS). Albert provides around-the-clock monitoring of many SLTT networks, analyzing over one trillion logs per month. Albert is a cost-effective solution that uses open-source software combined with the expertise of MS-ISAC analysts and engineers to provide enhanced monitoring capabilities and notifications of malicious activity.

CIS also provides low-cost access to endpoint detection and response (EDR), fully managed by the MS-ISAC. SLTTs have access to their data to provide robust analysis, supported by our analysts and cybersecurity experts. EDR technology is particularly effective at detecting and mitigating activity based on behavioral patterns rather than static signatures. EDR is one of the single most effective security solutions in the market today. We continue to work with vendor partners to add features and capabilities to this service at no additional cost to members.

We encourage this Committee to recommend that all SLTT governments in Oregon, especially

any SLTT-owned or operated critical infrastructure facilities, join the MS-ISAC (membership is free) if they have not already done so, and begin to take advantage of the many no- and low-cost resources available today.

Additionally, we recommend that the state encourage all SLTTs to implement the CIS Critical Security Controls on all SLTT networks, specifically high value networks and systems, such as those trusted by or connected to critical infrastructure. The Controls should be implemented in priority order starting with Implementation Group 1. Our analysis shows that implementing the CIS Controls mitigates almost 90% of all intrusion techniques.[8]

The third recommendation is for the state to encourage SLTTs to become SecureSuite members, which is provided to SLTTs at no cost. SecureSuite allows access to the CIS Benchmarks for hundreds of products, including all major operating systems, and helps organizations build, verify, and test security configurations. Using CIS Benchmarks helps ensure that security is baked into the deployment of systems and not tacked on as an afterthought.

Conclusion

In conclusion, I would like to thank the Committee and the Oregon State Legislature for allowing us this opportunity to provide this information today and for considering our recommendations for securing the state and its constituent SLTTs. I welcome the Committee's questions either here today at the hearing or subsequent written questions for the record, and would be pleased to work with this Committee as an ongoing resource on how to implement these recommendations at little or no cost to Oregon taxpayers as well as other aspects of cybersecurity.

Thank you.

[8] The ATT&CK framework comprehensively lists tactics and techniques that an attacker could use at each step of an attack. Read more about MITRE ATT&CK here: https://attack.mitre.org/

Attachment A
Brief Biography of Theodore J. Sayers

Theodore J. Sayers
Director, Intelligence & Incident Response
The Center for Internet Security
https://www.cisecurity.org/

Theodore J. Sayers joined CIS in 2016 as the Elections Cyber Threat Intelligence Analyst, supporting the newly established EI-ISAC and later as the acting MS- and EI-ISAC Liaison Officer to CISA. Prior to his current role as the Director of Intelligence and Incident Response, he was the Manager of Cyber Threat Intelligence, where he rehauled the team's mission, focus, and tradecraft to better align with an SLTT catered and proactive threat intelligence model.

He is currently serving in his eighth year with the United States Navy Reserve, with five former years as a prior enlisted Intelligence Specialist and presently, three years as an Intelligence Officer. He holds a Master of Public Administration and a Bachelor of Political Science as well as numerous industry certifications in the areas of incident response, digital forensics, reverse engineering, penetration testing, and security leadership.