Testimony of Randy G. Rose
Senior Director, Cyber Threat Intelligence
Center for Internet Security
Meeting of the
Joint Legislative Committee on Information Management and Technology (JLCIMT)
Oregon State Legislature
via Microsoft Teams
Wednesday, September 22, 2021
8:00 a.m. PDT

Representative Nathanson, Senator Riley, members of the Joint Committee, thank you for inviting me today. My name is Randy Rose, and I serve as Senior Director of Cyber Threat Intelligence for the nonprofit Center for Internet Security, Inc. (CIS).[1] I directly support the Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of CIS, which serves as the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. I have spent most of my career in service to the government at the State and Federal levels, including 15 years with the Department of Defense in active duty, reserve, and civilian roles. I have specific experience in the area of Local Government and Utilities with the New York State Office of the State Comptroller, where I developed the first cybersecurity audit and assessment program for municipal-operated utilities, including water supply & wastewater treatment, power, and port control, which is not only still in operation today but which has evolved and grown to cover aviation, transportation, and more. I appreciate this opportunity today to share my organization's thoughts on the threats facing SLTTs 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 local governments and the utility sector today; and (3) respectfully make four recommendations.

(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 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; and (3) the CIS Critical Security Controls. Each of these 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 2002, 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 state, local, tribal, and territorial (SLTT) governments and Fusion Centers. Its membership includes all 56 states and territories, and more than 11,000 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 municipal airports. The MS-ISAC offers a number of cybersecurity solutions for free for SLTTs, including network intrusion detection monitored by the ISAC Security Operations Center 24x7x365 and a malicious domain block service that helps prevent attacks before they happen.

EI-ISAC.[3] Following the interference in 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 have over 3,000 total members, including the election vendor community.

The CIS Benchmarks.[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.

The CIS Critical Security Controls.[5] CIS is also 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 free to the public.

Many governments and private sector organizations around the world have seen the benefit of the CIS Controls and have endorsed or adopted them including the State of Oregon, whose cyber audit of the state police conducted last year by the Audits Division of the Office of the Secretary of State contained several recommendations of the CIS Controls.[6]

---

[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 here: https://www.cisecurity.org/cis-benchmarks/
[5] Find out more information about the CIS Controls and download them for free here: https://www.cisecurity.org/critical-controls.cfm
[6] https://sos.oregon.gov/audits/Documents/2020-17.pdf

(2) The scope of the cyber threats facing state and local government today

SLTT governments and associated organizations are at a higher risk of successful compromise by malicious cyber actors than many other organizations. And they are being actively targeted by cyber actors.

A significant amount of information about SLTTs is in the public domain, including in some cases the types and versions of technology they employ. Examples include the entirety of the elections process, how utilities such as water and electric are measured and monitored, and data related to taxation and collection. SLTTs generally operate within a model of open information sharing and access. Citizens should be able to search for information about themselves, their local officials, and their communities. At the same time, the closer a government is to the individual constituent, the less resources it has for protecting that information and the systems that support it. While large states, major cities, and high-profile public universities likely have dedicated cybersecurity staff on hand, the same is not the case for most SLTTs, particularly LTTs, across the United States.

By now, the threat to governments, businesses, and American citizens is well known. In the most recent Worldwide Threat Assessment, the U.S. Office of the Director of National Intelligence concluded that "Cyber capabilities . . . are demonstrably intertwined with threats to our infrastructure and to the foreign malign influence threats against our democracy."[7] The report focuses on state actors yet draws a connection between many cybercriminal organizations and the countries which provide these organizations benefits, such as safe haven and freedom from prosecution. Ultimately, as a targeted organization, it may not matter if the perpetrator is a state actor, a criminal, or an insider. The potential impact is the same.

Additionally, Akamai reported observing more than a 100% increase in year-over-year phishing email attacks from 2019 to 2020.[8] We have observed cybercrime explode in the last few years, with over 4 thousand ransomware attacks in the U.S. alone each day resulting in over 2,400 SLTT victims in 2020. The average ransom demand has skyrocketed from around $5 thousand in 2018 to over $200 thousand per instance in 2020 and growing. This year alone, cybercrime is predicted to cost more than $6 trillion globally.[9]

No organization is immune. Recent attacks on technology service providers and supply chains, such as SolarWinds, Microsoft Exchange, and Kaseya, have put hundreds of thousands of organizations at risk simply for being a customer. SolarWinds revealed that approximately 18,000 of its customers had been exposed. Those customers ran the gamut from large businesses to Federal agencies, U.S. Department of Defense and the U.S. Department of Homeland Security, to municipal governments and associated organizations such as state hospitals, K-12 schools, and public universities.[10] The use of four separate zero-day exploits—attacks against previously unknown vulnerabilities—against Microsoft Exchange gave attackers full

---

7 https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

8 https://www.akamai.com/blog/trends/observed-changes-to-the-threat-landscape-in-2020

9 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

10 See, for example, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

administrator access to email servers and exposed user emails and passwords for users of an estimated 250,000 servers around the globe, including 30,000 in the U.S. alone. While the initial attack was attributed to state actors from China, cybercriminals leveraged the chaos to deploy ransomware on unpatched victims within days of the public disclosure of the attack. Indeed, the largest impact to SLTTs in these instances is often the follow-on cybercriminal activity due to delays in installing patches and mitigations in a timely fashion.

Some recent attacks on critical infrastructure have become major news stories due to their widespread impact. Two examples are the cyberattacks 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. The good news is that few critical infrastructure attacks are sophisticated enough to actually affect the operational technology itself. 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.

There certainly are cases where the control systems technology is actually the target of the attackers, such as the attack on the water system in Oldsmar, Florida, in February of this year. In this case, an attacker attempted to poison the water supply by increasing the amount of sodium hydroxide in the water supply 100-fold. While this is certainly frightening and of utmost concern, most instances of attacks that impact control systems are not of this flavor.

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. Nonetheless, in all cases, the operation environment was severely impacted. Likewise, all of these attacks were conducted by criminal actors interested in a big payday. Each of these attacks involved ransomware, which is arguably the fastest growing threat across all sectors, SLTTs included, today. And while neither of these organizations are SLTTs, the second- and third-order effects of the attacks sent ripples through their local community and beyond. For example, the Colonial Pipeline attack affected fuel supplies to municipal airports up and down the east coast. The MS-ISAC Cyber Threat Intelligence team and DHS Intelligence & Analysis recently completed a joint analysis product that concluded with the following assessment based on observed trends and global conditions: "We assess that ransomware attacks targeting US networks are likely to increase in the near and long term because cybercriminals have developed effective business models to increase their financial gain, likelihood for operational success, and anonymity."

In July, the same group behind the attack on JBS Foods successfully conducted a cyberattack on a private information technology firm, Kaseya, which spread through a software update in the company's remote management and update tool. Kaseya has over 40,000 clients, many of whom are local governments. Over two months later, the full scope of the attack is still being assessed and it looks as if Kaseya's rapid response actions limited the damage; however, this attack is directly in line with expected trends.

Despite some groups claiming that they will not target local governments, hospitals, schools, and critical infrastructure, these networks continue to be attractive targets for criminals. Part of this may be due to the evolution of the ransomware-as-a-service model, whereby different

groups or individuals design and develop ransomware as those who deploy it. Affiliates subscribe to a given developer's network for a share of the profits of ransom payments. Therefore, the developers may not intend to hit specific targets, but once they have "sold" the use of the tool to affiliates, they may have limited control over how it is deployed.

This is of specific concern to defenders of SLTTs for a few reasons: (1) keeping key systems isolated or wholly disconnected from the Internet is not practical, even in the case of critical infrastructure; (2) a ransomware infection will deny access to systems that could be essential in monitoring, administering, and controlling critical data and services; (3) the criticality of systems and networks 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 and hospital networks targeted as the goal of the actors is a quick payday, and few organizations have the uptime requirements as those in these two sectors. Additionally, prominent—either by size or budget—municipalities and schools are likely to see increased targeting from ransomware groups due to publicly available data related to tax income and budgets as well as the pressure on victims to pay to avoid a media scandal. A prime example is Broward County School District in Florida, which suffered an attack in early 2021 after attackers learned of the district's massive budget. The District refused to pay the $40M dollar ransom which led attackers to leak nearly 26,000 files on the Internet after dropping their demand to $10M.

Thinking beyond ransomware, state actors and criminal actors may have specific interest in targeting SLTT networks, especially critical infrastructure and higher education, for a variety of reasons. Those can include espionage, intellectual property theft, destruction, delay, and even influence operations. In many cases, it is not immediately obvious if an actor is a criminal actor or aligned with a foreign state; and unfortunately, there is a spectrum of state responsibility that can include the state encouraging criminal activity by actively ignoring it. In most cases, attributing the attack to a specific group or individual actor is not important to the victim. However, understanding the intentions and capabilities of cyber actors is important for policy makers and strategic decision makers, such as the members of this Joint Committee.

SLTTs, particularly smaller, underserved LTTs, cannot make the necessary changes in their environments or bring in the resources they need without your help. They need guidance, support, and real change from the top down. It starts with recognizing that malicious cyber actors will increasingly target networks and systems aligned with Oregon's government institutions, especially those deemed as useful to gain a financial, political, social, or military advantage. And because SLTTs in Oregon are increasingly reliant upon Internet-connected devices, we should expect to see an increase in successful attacks until we adapt a true culture of cybersecurity.

(3) Recommendations

Resourcing is a key issue in the defense of SLTT networks across the nation. Key hurdles include obtaining and retaining qualified security professionals, educating existing staff, and procuring security tools within well documented budget limitations. A less visible issue, but arguable as important, is the need for a culture shift among leaders that prioritizes cybersecurity and bakes it into strategic decision-making, facilitates building capacity for cybersecurity projects and capabilities, and reduces overall risk to the systems, data, and people that are dependent on internet-connected technology.

The MS-ISAC can help. At the MS-ISAC, we recognize that SLTT governments are faced with a lot of problems to solve with little help and even fewer resources. Therefore, the following recommendations are designed to be implemented with little or no additional cost, using the people and capabilities already available at the local level.

Nearly a quarter of all non-Defense critical infrastructure in the U.S. is owned and operated by SLTT governments. There is work that needs to be done to protect this infrastructure and it must be prioritized due to the potential for catastrophe and loss of life that could follow a successful attack.

The first is for the state to recommend that all SLTT organizations, including SLTT-owned or operated Critical Infrastructure facilities, schools, and healthcare organizations, join the MS-ISAC if they haven't already done so. Compared with the other 49 states, Oregon is in the middle of the pack with regard to current membership with 212 members statewide. Compared with some of your closest neighbors, Oregon lags behind Washington and California, while beating Idaho and Nevada. Membership is free to all SLTT organizations and, as mentioned above, the MS-ISAC helps provide a foundation for cybersecurity for its members, which allows them to free up resources for other priorities. The MS-ISAC runs a 24x7 cybersecurity operations center that provides: (1) cyber threat intelligence related to ongoing or impending threats relevant to SLTTs, and coordinated with DHS, facilitating proactive defense; (2) real-time monitoring and early warning notifications containing specific incident and malware information that may affect members; (3) incident response support; and (4) various other benefits, including educational services and managed security services that help reduce overall risk, all at no cost to members.

In addition, MS-ISAC provides around-the-clock monitoring services ("Albert") of many SLTT networks, analyzing over one *trillion* logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS-ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. Furthermore, the MS-ISAC provides free Malicious Domain Blocking & Reporting and Endpoint Detection & Response services to its members. Taking advantage of these free services can help significantly reduce risk associated with ransomware and other critical threats, and allow SLTTs to focus on more localized priorities.

The second recommendation is to implement the CIS Controls on all networks trusted by or connected to critical infrastructure, in priority order, starting with Implementation Group 1.

Our analysis shows that implementing the CIS Controls mitigates approximately 83% of all attack Techniques found in the industry standard MITRE ATT&CK Framework[11] and 80% of targeted intrusion techniques.

The third recommendation is to deploy hardened images, such as the CIS Benchmarks, on all applicable systems, business and operational, and maintain these systems in their secure configurations. Using Benchmarks helps ensure that security is baked into the deployment of systems and not tacked on as an afterthought.

The fourth recommendation is to conduct regular audits of operational technology, control systems, and other critical infrastructure technology to ensure controls are not being bypassed, system usage is in line with expectations, and no unauthorized or otherwise unexpected activity is occurring in the network. Examiners from existing state and local agencies can easily be trained in what normal looks like and quickly find deviations from the norm.

Conclusion

I would like to thank the Joint Committee and the Oregon State Legislature for allowing the MS-ISAC this opportunity to speak with you today and for considering our recommendations. We recognize that you have a lot of options for outside expertise, and there is no better time to seek it than now. Combined with the evolving threat landscape, the recently Senate-passed bipartisan infrastructure bill includes a $1B grant program for states and local governments to strengthen cybersecurity infrastructure against ransomware and other major cyber threats. In light of this bill and its likely passage, the MS-ISAC is currently working with the National Association of State Chief Information Officers (NASCIO), the National Governors Association (NGA), the National Conference of State Legislatures, and other key stakeholders on ways we can assist any SLTT interested in applying for a grant. Our aim is to provide guidance and assistance to make the program as effective as possible and reduce stress for interested applicants.

I welcome the Committee's questions either here today or subsequent written questions for the record, and would be pleased to work with the Committee as an ongoing resource on how to implement these recommendations and provide additional cybersecurity services for the benefit of Oregon taxpayers. Thank you.

[11] 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
Biography of Randy G. Rose

Randy G. Rose
Senior Director, Cyber Threat Intelligence
The Center for Internet Security
https://www.cisecurity.org/

Randy G. Rose joined CIS as the Director of Cyber Threat Intelligence for the Center for Internet Security (CIS) in June 2020 and was promoted to Senior Director in March 2021. He has been a public servant in varying capacities since 2003 when he enlisted in the United States Air Force. Prior to joining CIS, he was a Department of Defense (DOD) civilian, running the largest Security Operations Center (SOC) in Europe for the Defense Information Systems Agency (DISA). While at DISA Europe, he earned the George Hoffman Civilian Leadership Award and the Outstanding Team of the Year award. He moved to Germany from Hampton Roads, Virginia where he had spent years building the DOD's first team dedicated to providing intelligence support to Defensive Cyber Operations (DCO). As the Deputy Intelligence Officer for the Navy Cyber Defense Operations Command (NCDOC) in Suffolk, VA, Randy oversaw the operations of over 100 sailors and civilians, led incident response efforts on 7 named operations, drove the design and implementation of a $2M digital forensics and malware analysis enclave, and brought innovative solutions to bear including cloud browser isolation, saving hundreds of millions of dollars in incident response costs per year.

He has previously supported the Defense Intelligence Agency, the NY State Comptroller's Office, and the NY Air National Guard. While at the NYS Comptroller's Office, he developed and implemented the first cybersecurity audit and assessment program for municipalities and special districts as well as the first cybersecurity assessment program for municipally-owned Operational Technology, including energy, water, and port control systems.

He holds a Master's of Science in Cybersecurity and a Bachelor's in Anthropology with a focus on Human Biology and Forensics. His independent research focuses on health sector cybersecurity, physical security, legal and ethical concerns in virtual communities, and future technologies, particular as they pertain to the humane use of technology.