

# Cybersecurity Quarterly

## Looking Back, Looking Ahead

**Winter 2024/25**


**Expert Predictions on What We Can Expect in the Cybersecurity Industry in 2025**

**Current Trends and Threats Facing Critical Infrastructure and Improving Their Defenses Against Future Threats**

**Balancing Security and Innovation When Adopting APIs in State and Local Government**

**New Resources to Help Implement the Security Best Practices Contained in the CIS Controls v8.1**

As we wrap up another eventful year in the cybersecurity industry, we take a look back at the industry trends, security threats, and new developments that shaped 2024, as well as look forward to some factors we can expect to dominate our conversations in 2025



**Increase your  
cyber maturity.  
Decrease your  
cyber risk.**

**Learn about the  
Cybersecurity Assistance  
Services Program.**



**MS-ISAC<sup>®</sup>**

Multi-State Information  
Sharing & Analysis Center<sup>®</sup>

**Learn More**

# Contents

## Featured Articles

<b>12 CIS Experts' Cybersecurity Predictions for 2025</b>	<b>3</b>
Senior leaders at CIS offer up their best insights and predictions on what they expect the cybersecurity industry will be focused on in the coming year	
<b>Cybersecurity Trends, Threats, and Future Hybrid Threats: Challenges to SLTT Critical Infrastructure</b>	<b>9</b>
A look at the evolving trends and vulnerabilities facing critical infrastructure organizations and key resources that can help them strengthen their cyber defenses	
<b>Securing the Digital Future: The Critical Role of API Security in Local Governance</b>	<b>12</b>
As state and local governments continue to adopt APIs to modernize and improve their digital services, adapting their security strategies is crucial to ensure trust and safety is balanced with innovation	
<b>New Supporting Resources to Help Implement CIS Critical Security Controls Version 8.1</b>	<b>16</b>
New resources from our Security Best Practices team to help organizations successfully adopt the new standards and guidelines of the CIS Controls v8.1	

## Quarterly Regulars

<b>Quarterly Update with John Gilligan</b>	<b>1</b>
<b>News Bits &amp; Bytes</b>	<b>2</b>
<b>Cyberside Chat</b>	<b>14</b>
<b>ISAC Update</b>	<b>20</b>
<b>Event Calendar</b>	<b>23</b>

Cybersecurity Quarterly is published and distributed in March, June, September, and December. Founded MMXVII.

Published by Center for Internet Security, 31 Tech Valley Drive, East Greenbush, New York 12061

For questions or information concerning this publication, contact CIS at [info@cisecurity.org](mailto:info@cisecurity.org) or call 518.266.3460

© 2025 Center for Internet Security. All rights reserved.

## Winter 2024/25 : Volume 8 : Issue 4

**Editor-in-Chief**  
Michael Mineconzo

**Supervising Editor**  
Laura MacGregor

**Copy Editors**  
Aaron Perkins  
David Bisson

**Staff Contributors**  
Brian de Vallance  
Stephanie Gass  
James Globe  
Kelly Morris  
Sharon Shoemaker  
Valecia Stocchetti  
Aaron Perkins

# A Partnership for State, Provincial, Local, Tribal, and Territorial Government

The SANS Institute and Center for Internet Security Partnership Program

## Improving Your Security Posture

Cyberthreats appear as fast as a mouse click in today's environment. Your best defense is an educated workforce. Eligible organizations use this Partnership Program to allocate technical cybersecurity and security awareness training to their employees, taking advantage of highly discounted rates on superior training to protect national security.

### Special Offer:

For a limited time, save more than 50% when you purchase SANS technical and security awareness training through our partnership purchase windows. Special discounts are available:

### Winter Program:

**December 1 – January 31**

### Summer Program:

**June 1 – July 31**

Make a positive impact on your cybersecurity protection. Get the training you need at an affordable cost.

Technical training is a critical component for adoption of core security awareness concepts. Compliance and behavior change becomes difficult for non-technical individuals without the proper content. SANS Security Awareness offers a comprehensive solution for end users and individuals of all levels with expert- authored content. Created by a trusted global network of cybersecurity professionals, this Partnership Program includes several key Security Awareness products:

- **End User** - Comprehensive security awareness training for all computer users based on the Critical Security Controls
- **Healthcare** - Computer-based security awareness training tailored to healthcare organizations
- **Developer** - Train your developers in secure coding techniques and how to recognize current threat vectors in web applications
- **ICS Engineer** - Rigorous computer-based training for those interacting or operating with Industrial Control Systems
- **Phishing** - Test your employees through phishing simulations consistent with real-world attacks
- **CIP** - Relevant training addresses NERC CIP reliability standards for the utility industry

A Smart Approach to Security Awareness and Training

[www.sans.org/partnerships/sltd](http://www.sans.org/partnerships/sltd)



# QuarterlyUpdate with John Gilligan

**"At the Center for Internet Security® (CIS®), we are also observing that threat actors are increasingly using multiple modes of attack to achieve their objectives"**

As I write this, winter has finally arrived in the D.C. area. Our very mild fall has given way to snow and freezing temperatures across much of the nation. Shorter days and cooler temperatures are with us for a few months.

We are now past the 2024 General Election. The incoming Administration is promising to implement some significant changes. It is not clear if these changes will extend to addressing the growing vulnerability that our nation faces from a variety of threats.

The recent election showcased the progress that has been made in improving the cyber defenses of our election systems. It is not that cyber threats have diminished; to the contrary, the number of threats continues to increase. In the recent election, there were no major cyber disruptions. Since 2016 when there were cyber attacks focused on voter registration systems, election offices have been focused on strengthening their cyber defenses. The Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®) has also made significant contributions in this area.

Another major conclusion from the recent election is that the nature of the threats continues to evolve. In 2016, the primary threat was cyber attacks, while in 2020, the primary threat was use of misinformation to influence voters. In 2024, the primary threat was physical disruption, specifically bomb threats, swatting, white powder envelopes, and doxing. At the Center for Internet Security® (CIS®), we are also observing that threat actors are increasingly using multiple modes of attack — cyber attacks, information operations, and physical disruption — to achieve their objectives. Simultaneously, the use of multiple threat modes, oftentimes referred to as "hybrid threats" or "multidimensional threats," is growing rapidly.

In the 2024 election, the coordination and planning efforts by election officials with their law enforcement and public safety colleagues permitted them to respond quickly and without major disruption to voting or vote counting and certification of results. Cooperation among cyber experts and those responsible for responding to physical or information operation threats will be increasingly important in the future.

For this quarter's issue, we'll look back and evaluate the past year in cybersecurity. The articles highlight the focus of the industry and CIS in 2024 as well as indications of what is to come next year.

To start, a number of senior leaders from CIS provide their insights on what cybersecurity topics, threats, and technologies we can expect to dominate our conversations in the coming year. In a subsequent article, James Globe, CIS Vice President of Strategic Cybersecurity Capabilities, examines the emergence of hybrid threats and the implications for U.S. State, Local, Tribal, and Territorial (SLTT) organizations and their systems — in particular, critical infrastructure systems including industrial control systems.

Then, Valecia Stocchetti, Brian de Vallance, and Sharon Shoemaker from the CIS Security Best Practices team discuss the resources that CIS has published over the past year to support implementation of CIS Critical Security Controls (CIS Controls) v8.1.

Another article by Kelly Morris, Director of Maturity Services in CIS's Stakeholder Engagement Organization, looks back at the new initiatives that the ISAC Member Engagement Team implemented in 2024, including regional events, collaborative efforts with the Office of the National Cyber Director focused on K-12 schools, and workshops with the National Center for State Courts.

Additionally, our partners at Akamai gives us a glimpse at some of the emerging threats that we can expect to see affect local government in 2025, particularly around APIs.

I hope you enjoy this quarter's issue. Have a great winter season!

Best Regards,

John M. Gilligan  
President & Chief Executive Officer  
Center for Internet Security



## CIS and Google Provide Practical Approach to Cloud Adoption for SLTT Governments

Migrating to the cloud can be a game-changing catalyst for U.S. State, Local, Tribal, and Territorial (SLTT) organizations. However, SLTTs need to also factor in security and compliance of their assets when they start planning their cloud adoption. This can

be challenging, especially if the organization is new to using cloud environments. To help these organizations, The Center for Internet Security® (CIS®) collaborated with Google to develop a pragmatic approach to cloud adoption, migration, and security for SLTT government organizations. To learn more about the report and to download a copy, please visit [our website](#).



## CIS Releases Results of 18-Month Study of U.S. Tribal Cybersecurity

The Center for Internet Security® (CIS®) released the 2024 MS-ISAC® Tribal Sector Cybersecurity Report, a publication which shares the results of an 18-month study into the cybersecurity landscape of U.S. Tribal organizations.

"This report includes lessons learned, strategic and tactical recommendations, and expert analysis into today's cyber threat landscape, and I'm eager to share such a fantastic report with the Tribal community," said Greta Noble, Director of Community Engagement at CIS.

To learn more about the report and to download a copy, please visit [our website](#).



## CIS CyberMarket®

### CIS CyberMarket® Announces New Vendor

CIS CyberMarket has added a new vendor to its list of valued partners: Enzoic. Enzoic provides easy-to-use authentication solutions to [maintain password policy compliance](#) and [prevent account takeover](#). CIS CyberMarket is a marketplace specifically designed to help connect U.S. State, Local, Tribal, and Territorial (SLTT) government organizations with rigorously-vetted, cost-effective cybersecurity solutions from industry-leading vendors. To view all of our current offerings, please visit the [CIS CyberMarket webpage](#).



## The Nationwide Cybersecurity Review (NCSR) is Now Open to U.S. SLTTs

The NCSR is a no-cost, anonymous, annual self-assessment. All U.S. States (and related agencies), Local governments (and departments), Tribal nations, and Territorial organizations (SLTTs) are encouraged to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs, and it is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). It is now open for submissions through February 2025.

Using the results of the NCSR, DHS delivers a bi-yearly anonymous summary report to the U.S. Congress providing a broad picture of the cybersecurity maturity across SLTT communities. The MS-ISAC and EI-ISAC also release an annual report that can help decision makers understand how their risk tolerance and maturity compare with similar organizations and facilitate self-comparison from year to year. To view the 2023 NCSR Report, please click [here](#).

Learn more about the NCSR and get started on assessing your organization's cybersecurity program on [our website](#).

# 12 CIS Experts' Cybersecurity Predictions for 2025

After another tumultuous year in the cybersecurity industry, we asked a dozen experts and senior leaders at CIS to predict what we can expect to be the topics of conversation for 2025

By CIS Staff

The [2024 general election](#) . . . the [CrowdStrike Falcon outage](#) . . . [insider threats from nation-state actors](#) — these developments created new risks for organizations like yours in 2024. In doing so, they shifted the conversation around your cybersecurity priorities going forward.

There's so much change in the cybersecurity field to decipher. Where do you focus your efforts?

To put this new year into context, we spoke to a dozen experts at the Center for Internet Security® (CIS®) about their cybersecurity predictions for 2025. Here's what they had to say.

**Marci Andino | VP of the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®)**

While the increase in attention generated by a presidential election is over, election officials will continue to experience the impact of [generative artificial intelligence](#) (GenAI). GenAI makes it easier, faster, and more economical to create higher quality phishing emails. But it's not all bad news. There will likely be more positive uses of the technology, as well.

The EI-ISAC will also continue to adapt to multidimensional threats in order to better meet the needs of our election members. Cyber attacks on critical election infrastructure can be combined with information operations, physical attacks, and [election disruption tactics](#) to impact election operations.

**Sean Atkinson | CISO**

**Zero Trust Enablement with the Focus for 2025 on Identity:** The emphasis on unauthorized access and

There's so much change in the cybersecurity field to decipher. Where do you focus your efforts? To put this new year into context, we spoke to a dozen experts at the Center for Internet Security® (CIS®) about their cybersecurity predictions for 2025.

privilege escalation will act as a catalyst to drive a robust assessment of identity management and drive adoption of [zero trust](#) security models.

**AI-Enabled Attack and Defense:** We will continue to see new artificial intelligence (AI) capabilities and maturity in this space as attackers integrate this capability into sophisticated attack strategies and defenders/vendors integrate better models into defensive capability.

**Supply Chain Risk Management:** An increased focus on assessment strategies for vendor due diligence, vendor alignment to more robust security compliance frameworks, a start of the "shift left demand" from the customer base, as well as organizations and thought leaders building governance assessment models for AI integrations into products and services.

**Jason Emery | Director of Cybersecurity Advisory Services**

**AI-Assisted Cybersecurity Tools:** I believe we will see the continued evolution of AI-assisted cybersecurity

tools that help offset the lack of cybersecurity professionals in smaller U.S. State, Local, Tribal, and Territorial (SLTT) government organizations. These tools will provide operations-oriented IT staff the ability to manage and secure their environment even while overwhelmed by the daily tasks of “keeping the lights on.” Managed service providers (MSPs) and managed security service providers (MSSPs) will also leverage these tools to become nimbler and to stretch their limited human resources further when supporting their clients.

**Governance Focus in K-12:** In my work, I see many small- to medium-sized K-12 school districts starting to focus more on formalizing their cybersecurity programs, including governance from the top down. Many district superintendents and school boards are realizing the importance of top-level support in these programs. A good cybersecurity program is not just an IT concern but is, in fact, a strong business concern. I see districts implementing proven cybersecurity controls like the [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework \(CSF\)](#) and the [CIS Critical Security Controls \(CIS Controls\)](#) more in the coming year to help them be strategic in their efforts and investments.

**IT-OT/ICS Convergence:** IT and Operational Technology (OT) / [Industrial Control Systems \(ICS\)](#) will continue to see more convergence. These systems are used to manage our [water](#), [wastewater](#), power, etc. Traditionally, these platforms have remained outside the IT environment. I see more of these systems being connected to the general network for remote management, additional capabilities, etc. This adds cybersecurity risk to these environments. We will see more emphasis being placed on proper vulnerability management, threat detection, and cybersecurity frameworks for OT/ICS environments. They key to success will be to take into account the unique nature of these systems to avoid affecting uptime negatively.

#### **Don Freeley | VP of IT Services**

**Zero Trust Advances in the Enterprise:** Embracing a zero trust approach to securing company assets, access, and systems will gain momentum in organizations of all size in 2025. Employees and customers demand access to resources and data from multiple locations and devices. Each link in the access chain needs to be treated as untrusted, with access and authorization continuously verified. Secure websites or VPNs, even with MFA enabled, are not enough to prevent unauthorized access, data loss, and exfiltration.

**Secure by Design Becomes Part of IT's DNA:** Recent high-profile security breaches will drive adoption of [secure by design](#) principles in IT projects. The idea



that security can be bolted on to a service or project at the end has shown itself to be hard and inefficient. Incorporating security, compliance, and governance into early stages of a design leads to better overall outcomes and helps foster a culture of security across the organization. IT organizations will accelerate the move in this direction in 2025.

#### **Stephen Jensen | Sr. Director of Plans, Programs, & Exercises**

2025 is bringing with it more connected devices than ever before. The Internet of Things (IoT) has revolutionized how organizations collect data about the day-to-day lives of their customers and employees. The intersection of conventional networks with wirelessly enabled devices of all sizes and types creates new avenues for attack as well as new areas of focus for security professionals. Securing these connected devices by using network segmentation, improved network protocols meant for these types of connections such as Wi-Fi HaLow, and ensuring that your devices are [patched and updated](#) when available will help to keep your environments secure.

#### **Angelo Marcotullio | CIO**

Training and adhering to basic cybersecurity practices ensure that even non-technical staff can recognize and mitigate risks. Cyber attacks such as phishing, ransomware, and malware often exploit human errors, making employees the first line of defense. By focusing on these basics, employees help safeguard the organization's reputation, financial stability, and customer trust. Moreover, prioritizing cybersecurity fosters a culture of responsibility and [awareness](#) across the workforce. Employees who are vigilant about spotting suspicious activities and following security protocols not only protect themselves but also contribute to the organization's overall resilience. This collective effort minimizes



the likelihood of successful cyber attacks and demonstrates the organization's commitment to safeguarding its stakeholders. Empowering all employees to recognize and report potential cybersecurity attacks can lead to the prevention of cyber attacks.

### Lee Myers | Sr. Director of Security Operations

**Consolidation of Operations:** For many years, there has been a rush to spend cybersecurity funding to bring in the latest and greatest technology to aid in [cyber defense](#) efforts against an ever-evolving cyber attack ecosystem. Organizations' technology footprint now exceeds their ability to successfully leverage the tools "in house," with them relying on third-party consultants or service providers to utilize these tools and leverage the collected data on their behalf. As expertise grows within these organizations and a more mature cyber strategy emerges that aligns with business or organization goals, we will see a reduction in redundant or unused technology within individual organizations. This will lead to increased efficiency and impact from the tools that remain, with resources being reprioritized for their use and the value that they bring to the organization.

### Lee Noriega | Executive Director of Cybersecurity Services Organization and Acting General Manager of Sales and Business Services

Going into 2025, the security risks of AI will continue to be a huge area of concern for many organizations.

- Cybercriminals will continue to leverage AI to enhance the sophistication and scale of their attacks.
- AI-Generated phishing emails and adaptive malware will make it increasingly difficult for traditional security measures to detect and mitigate threats.

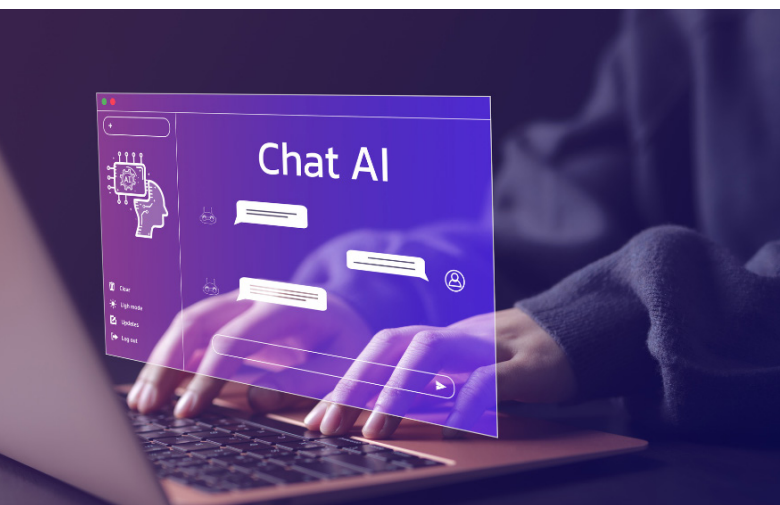
- AI will contribute to the evolution of ransomware, increasing the speed and precision of these attacks as well as making them more difficult to defend against.
- The combination of social media and generative AI will enable more sophisticated scams and impersonations.
- As AI tools become more integrated into business operations, there will be a growing risk of data breaches caused by improper use of these tools.

### Randy Rose | VP of Security Operations & Intelligence

**Increased Uses for Quantum Outside of Research:** In 2025, expect to see application of quantum computing outside of the university research lab. Advances in quantum are expected to challenge current cybersecurity measures by potentially breaking common cryptographic algorithms. In response, there will be a surge in adopting quantum-resistant algorithms (aka post-quantum cryptography) to protect sensitive data across all industries. Additionally, quantum computing will enhance threat detection and predictive analytics; it will be marketed as a means to enable a shift from being reactive to being proactive. In software development, quantum computing will drive innovation in algorithm design, improving efficiencies in code execution and problem-solving capabilities. Expect well-resourced early adopters to start implementing soon and less resourced followers to face technical and financial challenges in updating systems to keep up pace.

**Evolution of IoT and Edge Computing:** The industry continues to move from the cloud to the "fog" of edge computing, placing data processing closer to the data source and even using crowdsourcing techniques of other nearby devices. This is going to put an increased focus on IoT as an increasingly attractive target for attackers, as one of the biggest beneficiaries of edge computing is the IoT device handling real-time data. IoT devices are now ubiquitous; they're found throughout homes and businesses globally, including smart appliances, HVAC systems, solar and other power systems, and smart speakers, to name a few. As the attack surface for IoT grows, so too will the need for IoT security tools, frameworks, and [best practices](#).

**Focus on Socio-Political Impacts of Emerging Technology:** While AI and machine learning (ML) have been around for a long time now, their use historically was mostly hidden from the public consumer. That changed in November 2022 with the public release of ChatGPT followed by other large language models

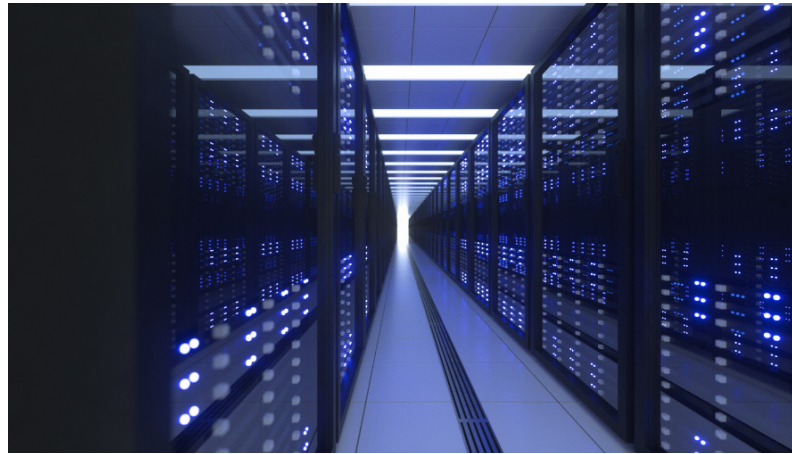


(LLMs). We're now leaving the honeymoon phase and beginning to shift focus onto what we've learned these past two years on the social, political, and technical impacts of GenAI. Expect more research on the impact of GenAI on everyday life, the use of GenAI to augment skills that once took years to hone (such as coding), and the democratization of creative works. There will be significant challenges to intellectual property claims and authenticity which we may start to see play out in court in 2025. Based on the way the models are trained, some LLMs have been shown to widen existing gaps in equity and increase digital repression. While GenAI has the potential to enhance learning and accessibility, without proper oversight, it risks deepening the digital divide, supercharging disinformation and information operations campaigns, and amplifying global concerns around human rights.

### **Marcus Sachs | SVP, Chief Engineer**

**Artificial Intelligence:** In 2025, artificial intelligence (AI) will play an even larger role in cybersecurity, both for good and bad. Attackers are likely to use AI to automate attacks, create adaptive malware, and avoid traditional detection methods. Unlike manually controlled attacks, [AI-powered adversaries](#) will use adaptive algorithms to change and carry out attack strategies in real time. These strategies could adjust based on what they detect and exploit, making it harder for defenders to keep up. Meanwhile, [defenders will also increase their use of AI](#) to improve threat detection, anomaly spotting, and predictive analysis. This AI "arms race" will redefine how attackers and defenders tackle cybersecurity.

**Compliance and Regulation:** As AI systems become more common, cybersecurity issues related to data privacy, manipulation of AI models, and misuse of AI-generated content will grow. To address this, compliance frameworks will be introduced to ensure organizations secure their AI training data, model accuracy, and interactions with users. This new focus on "AI security compliance" will push companies to improve defenses around AI models, reducing risks of disinformation, theft of intellectual property, and misuse of sensitive data in AI systems. Beyond AI, traditional regulatory actions will impact critical infrastructure, with governments likely to enforce minimum cybersecurity standards and response protocols to boost resilience against physical and cyber threats. Expect new policies requiring cybersecurity education and proactive risk assessments for critical infrastructure to mitigate major risks. [Cyber-Informed Engineering](#) principles may gain traction as an essential tool for embedding resilience into critical systems.



**Cloud Security:** With more organizations [moving data and operations to the cloud](#), there will be greater attention on cloud security and data location. In 2025, new laws may require that sensitive data stay within national borders, affecting how companies manage and store data across regions. This emphasis on data sovereignty will lead companies to adopt multi-cloud strategies to stay compliant with evolving regulations while ensuring flexibility and security. As businesses and critical services become increasingly dependent on cloud services, some countries may prioritize cloud availability in national emergency plans, recognizing that stable cloud access is mandatory for crisis management. This shift could lead towards the establishment of a new program like Cloud Service Priority (CSP), treating cloud infrastructure as important as utilities like electricity and telecoms.

**Zero Trust:** Zero trust architectures, which do not assume any inherent trust within or outside an organization's network, will likely become the default approach for cybersecurity in organizations with hybrid or remote workforces. As employees work from various locations on different devices, zero trust will gain importance for securing both on-premises and cloud environments. This approach will drive investments in identity and access management, endpoint security, and continuous monitoring technologies, changing how companies secure both internal and external access.

### **TJ Sayers | Director of Intelligence & Incident Response**

**A Bolstered Cybercriminal Market for Phishing as a Service Models:** AI-Driven tools have all but eliminated classic human errors within traditional social engineering activity. Typos and formatting mistakes in text-based phishing are increasingly rare, and advanced voice and video deepfakes are near-indecipherable from reality. Exploiting the human as an initial attack vector still reigns supreme, and customizable phishing kits under a fee-for-service model will lower the bar of entry for threat

actors and greatly increase their social engineering successes against end users.

My predictions from [last year](#) will also apply in 2025. Ransomware and associated extortion-based threats will undoubtedly remain the leading and most disruptive threat facing SLTTs, and blurred lines between threat actor groups will grow increasingly opaque.

### **Valecia Stocchetti | Sr. Cybersecurity Engineer, CIS Critical Security Controls**

**AI Embedded in Software:** AI has exploded in many ways over the past 1–2 years. This rise in the use and abuse of AI will likely continue to grow in 2025. Organizations will face many complex challenges because of this. For one, vendors will continue to embed AI features into their software and applications, producing a forcing-function for organizations to either adopt or drop these new features. In some instances, these AI features can't be turned off or removed. Organizations will need to be vigilant in what is acceptable risk in terms of using AI features. Questions to ask include the following: Where is my data being stored? Is it being kept confidential and is it protected? Am I still in compliance with certain regulations I need to comply with? Regulations on AI are still emerging. It remains to be seen whether end-organizations will be able to keep up with demands on the vendor side.

**AI-Based Threats:** On the other hand, AI-based threats will continue to grow, impacting both our personal and professional lives. Organizations will face an increase in [phishing attacks](#) created with AI, making them more lifelike and less like the former “Nigerian prince” email scams we once solely faced. This means that users will need to be even more observant and, more importantly, “think before they click.” According to the [2024 Verizon DBIR](#), human elements are still responsible for 68% of data breaches. While that figure may have fluctuated somewhat over the years, it still remains quite high. Organizations will need to continue to implement a defense-in-depth strategy in order to block these threats and prevent themselves becoming tomorrow’s news headline.

**AI For The Better:** While AI can pose all sorts of “doom and gloom” in the cybersecurity world, it can also do a lot of good. Depending on the technology, we can become more efficient at our jobs, reducing the need for manual work. For example, it can help us with intrusion prevention systems so that we can detect and prevent the less “noticeable” threats as well as reduce the rate of false positives. There is also the benefit of AI models learning from the data that is fed into the system, making it (hopefully) more effective.

Overall, AI will continue to spark innovation, bring about new threats, and continue to raise privacy concerns. As with anything in the field of technology, it's a balance between usability and security. This is why it is important for organizations to:

- Practice due diligence when it comes to vetting software vendors
- Consider the benefit that AI can bring and weigh it against the risk
- Keep up to date with emerging threats

### **Stay Current with Multidimensional Threats**

The predictions above are what stand out to us. They're not all-inclusive of everything that's changing in cybersecurity. If you think we missed something, let us know on [Twitter](#), [LinkedIn](#), or [Facebook](#).

You then need to focus on keeping up with all the changes discussed in this article. One of the ways you can do this is by taking a proactive approach to understanding new developments among cyber, physical, and hybrid threats. To simplify this process, we created ThreatWA™. It brings together the expertise of CIS analysts to illuminate emerging multidimensional threats that matter to you.

Ready to stay aware and protected with clear, actionable threat insights? Check out and subscribe to [ThreatWA](#) to get expert insights and trends to stay ahead of the latest cyber threats in 2025 and beyond.





Center  
for Internet  
Security®

# ThreatWA™

The **premiere** subscription summarizing threat-related activity across the globe.

Created by and available to cyber and physical security professionals.

**15-day free trial available**

**Learn More**

# Cybersecurity Trends, Threats, and Future Hybrid Threats: Challenges to SLTT Critical Infrastructure

Critical infrastructure within SLTT organizations has been rapidly adopting new technology to improve services, as well as become an increasingly common target for cyber criminals. Leveraging key resources from CIS can help address and alleviate these concerns.

By James Globe

The digital transformation of U.S. State, Local, Tribal, and Territorial (SLTT) organizations' critical infrastructure has significantly expanded the attack surface for cyber threats. From utilities and healthcare to transportation, elections infrastructure, and emergency services, SLTT operational technology (OT) and information technology (IT) systems are increasingly targeted by adversaries seeking to disrupt operations, compromise sensitive data, and erode public trust. Sophisticated threats, including ransomware, supply chain vulnerabilities, and hybrid attacks, demand a proactive approach to cybersecurity. By adopting advanced strategies like [CIS Critical Security Controls \(CIS Controls\) Implementation Group 1 \(IG1\)](#) and the [CIS Controls v8.1 Industrial Control Systems \(ICS\) Guide](#), SLTT organizations can build a robust defense-in-depth approach while addressing challenges like insider threats, cloud migrations, and shadow AI risks. This article explores key trends, threats, and actionable strategies for securing critical infrastructure within SLTT organizations.

## Cybersecurity Trends in SLTT Critical Infrastructure

### *Cloud Computing and Digital Transformation*

SLTT organizations are increasingly adopting cloud technologies to enhance efficiency, scalability, service reliability, and cost-effectiveness. However, this shift introduces new vulnerabilities, such as misconfigured systems and insecure APIs, necessitating robust cybersecurity measures. To address these risks, SLTT organizations must implement data encryption, data loss

Sophisticated threats, including ransomware, supply chain vulnerabilities, and hybrid attacks, demand a proactive approach to cybersecurity. By adopting advanced strategies like CIS Critical Security Controls (CIS Controls) Implementation Group 1 (IG1) and the CIS Controls v8.1 Industrial Control Systems (ICS) Guide, SLTT organizations can build a robust defense-in-depth approach

prevention technology, multi-factor authentication (MFA) integrated with zero-trust principles, and real-time behavioral analysis for endpoint and network monitoring.

Hybrid cloud configurations that integrate public, private, and secure government environments become a standard deployment model; advanced security frameworks are essential to protect sensitive data and ensure compliance with regulations like GDPR and HIPAA. Incorporating CIS Controls IG1, such as asset inventory and secure configurations, provides a solid foundation for mitigating risks associated with cloud adoption.

## ***Zero-Trust Security Architecture***

The zero-trust model is gaining traction as a critical security approach for SLTT organizations. It enforces least-privilege principles, continuous authentication, and system logs monitoring, ensuring that no user or device is trusted by default. Implementing zero trust involves network segmentation (or micro-segmentation), strong identity verification, and behavior-based analytics to detect anomalies in systems log files.

While zero trust is vital for securing modern networks, organizations should focus first on foundational security measures from CIS Controls IG1, which assure appropriate cyber hygiene activities. This includes securing administrative privileges, maintaining accurate hardware and software inventories, and regularly updating and patching systems.

## **Emerging Cyber Threats**

### ***Ransomware and Double-Extortion Attacks***

Ransomware remains a top threat. Nation-state actors are increasingly targeting SLTT critical infrastructure to disrupt services and demand ransom payments. Double-Extortion tactics, where attackers both encrypt data and threaten to leak it, add additional layers of complexity. Implementing CIS Controls IG1 can help mitigate these threats by ensuring regular backups, secure configurations, and network segmentation. SLTT need to assure recurring cyber hygiene activities combined with security awareness training, particularly for phishing attacks. Doing so is critical for preventing and/or lessening the impact of these attacks.

### ***Supply Chain Vulnerabilities***

Supply chain attacks exploit vulnerabilities in third-party vendors to infiltrate SLTT organizations' operational

technology and IT systems. SLTT organizations must vet vendors rigorously, require adherence to cybersecurity standards, have potential vendors fill out a risk questionnaire, and conduct regular audits. CIS Controls IG1 Safeguards, such as monitoring authorized hardware and software, provide a solid foundation for reducing supply chain risks.

### ***Insider Threats***

Insider threats, whether malicious or accidental, pose significant risks to critical infrastructure. Employees or contractors with access to sensitive systems or data can cause damage to SLTT organizations through negligence or deliberate actions. Adopting MFA with zero-trust principles, enforcing least-privilege access, and continuously monitoring user behavior are key strategies for mitigating insider threats.

## **Future Hybrid Threats**

### ***Cyber-Physical Integration Risks***

As operational technology (OT) systems become more integrated with IT networks, the risk of hybrid threats — those combining cyber and physical elements — increases for SLTT organizations. For instance, a cyber attack on ICS could disrupt power grids, transportation systems, or water treatment facilities. The CIS Controls v8.1 ICS Guide provides a defined pathway for securing OT environments, emphasizing inventorying control systems, managing vulnerabilities, and monitoring for suspicious activity. Organizations must also conduct regular penetration testing and develop incident response plans that address both cyber and physical risks.

### ***Shadow AI Risks***

The proliferation of shadow AI, unauthorized or unvetted AI tools and services, introduces new vulnerabilities, such as data leakage and compliance violations. To address this, organizations should:

- Maintain an inventory of all AI tools in use,
- Develop clear governance and acceptable usage policies for AI adoption, and
- Conduct regular audits to ensure compliance with security standards.

Integrating shadow AI tools into broader cybersecurity frameworks, such as CIS Controls IG1, and monitoring for suspicious activity ensures that these technologies are secure and compliant.



## Key Strategies for Resilience

### Leveraging CIS Controls IG1

CIS Controls IG1 focuses on essential cyber hygiene practices critical for securing SLTT organizations critical infrastructure. Key controls include:

- **Inventory and Control of Assets:** Keeping accurate records of hardware and software prevents unauthorized devices from compromising systems.
- **Secure Configuration:** Ensuring systems are configured securely reduces vulnerabilities.
- **Continuous Vulnerability Management:** Regularly scanning for and patching vulnerabilities minimizes the attack surface.
- **Controlled Use of Administrative Privileges:** Restricting privileged access limits the impact of insider threats and credential theft.

These basic measures are cost-effective and scalable, making them ideal for resource-constrained SLTT organizations.

### Leverage CIS Controls v8.1 ICS Guide

For critical infrastructure organizations with industrial control systems, the CIS Controls v8.1 ICS Guide provides tailored guidance for securing OT environments. Key recommendations include:

- Segmenting OT networks from IT systems to limit attack pathways,
- Monitoring ICS activity for anomalies and potential threats, and
- Ensuring regular updates and patching of ICS components to prevent exploitation.

By integrating ICS-specific controls with broader cybersecurity strategies, SLTT organizations with both OT and IT systems can protect both digital and physical assets.

### Incident Response and Resilience

Effective incident response is critical for minimizing the impact of cyber attacks. SLTT organizations must:

- Develop and regularly test incident response plans
- Establish communication protocols for public transparency during breaches

- Invest in threat intelligence sharing through platforms like Analyst1, as well as participate in indicators of compromise sharing with Information Sharing and Analysis Centers, like the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS-ISAC® and EI-ISAC®), to improve preparedness

A strong focus on resilience ensures that critical services can recover quickly from attacks, maintaining public trust and safety.

## Conclusion

The cybersecurity landscape for SLTT critical infrastructure is increasingly complex, driven by trends like cloud adoption, hybrid threats, and the integration of IT and OT systems. Emerging challenges, such as ransomware, supply chain vulnerabilities, and shadow AI, require organizations to adopt proactive and comprehensive strategies. Foundational measures from [CIS Controls IG1](#), complemented by the [CIS Controls v8.1 ICS Guide](#), provide a robust starting point for improving security. At the same time, addressing workforce shortages and fostering collaboration across sectors will be critical for long-term resilience. By prioritizing security, SLTT organizations can protect vital services, safeguard public trust, and adapt to an ever-evolving threat landscape.

.....

*James Globe, CISSP, is the Vice President, Strategic Advisor Cybersecurity Capabilities at the Center for Internet Security® (CIS®). Globe serves as the senior leader within Operations and Security Services (OSS) responsible for advising on strategic cybersecurity capabilities, cybersecurity workforce, data analytic analysis, frameworks, and emerging and enabling technologies for use by U.S. SLTT members.*

*He has more than 20 years in technology leadership, including extensive experience engineering signal intelligence mission systems, workflow management systems, financial and banking systems, modeling and simulation systems, and web-based information portals for top-tier banking and defense contracting organizations, including Bank of America, SAIC, BAE Systems, and L3 Harris Technologies.*

*Globe earned a Bachelor of Science in computer science and mathematics from Georgia State University. He also holds a Master of Science from John Hopkins University in telecommunications and security engineering.*

# Securing the Digital Future: The Critical Role of API Security in Local Governance

Application Programming Interfaces (APIs) have grown in popularity with SLTT organizations looking to improve their digital services, but adopting this technology requires organizations to adapt their security strategies accordingly

By Brian S. Dennis

In today's increasingly digital world, local governments are harnessing technology to enhance public services, streamline operations, and engage more effectively with citizens. At the forefront of this transformation are Application Programming Interfaces (APIs) — critical tools that enable seamless communication and data sharing between software systems. While APIs unlock innovation and efficiency, they also introduce significant security vulnerabilities if not properly safeguarded. Robust API security is no longer optional; it is an essential component of responsible governance.

## The Role of APIs in Local Governance

Local governments manage vast amounts of sensitive data ranging from citizens' personal information to critical infrastructure details. APIs act as the conduits for this data, enabling systems to work cohesively and power digital services. However, an unsecured API can become a gateway for cybercriminals, exposing sensitive information or disrupting essential operations.

For example, an unsecured API might leak Social Security Numbers, tax records, or property data, leading to identity theft or financial fraud. Even more alarming, breaches involving operational systems — such as traffic management or emergency services — could jeopardize public safety on a large scale.

## Growing Cybersecurity Threats

Cyber attacks on public-sector entities are becoming more sophisticated and frequent. APIs, as some of the most exposed points in a digital ecosystem, are prime targets for attacks such as:

At the forefront of this transformation are Application Programming Interfaces (APIs) — critical tools that enable seamless communication and data sharing between software systems. While APIs unlock innovation and efficiency, they also introduce significant security vulnerabilities if not properly safeguarded..

- **Injection Attacks:** Inserting malicious code into API queries to manipulate or exploit systems
- **Data Exfiltration:** Extracting sensitive data by exploiting weak validation processes
- **Distributed Denial of Service (DDoS):** Overwhelming APIs with traffic to disrupt service.

For local governments, these attacks could cripple essential services, such as water supply, waste management, and emergency response systems. Beyond operational disruptions, such breaches could also result in compliance violations, reputational damage, and hefty fines.

## The Case for API Security

Investing in API security is crucial for safeguarding public systems and citizen data. Unprotected APIs can



inadvertently expose personally identifiable information (PII), leading to compliance violations and legal consequences. Furthermore, maintaining public trust is paramount; a high-profile breach could erode confidence in government services.

Additionally, gaining visibility into all APIs is crucial to identify potential vulnerabilities, misconfigurations, or unauthorized access points that could expose a network to cyber threats. It enables proactive monitoring and response, ensuring the security and resilience of critical systems and data.

For instance, a compromised API in a public transit system could expose user location data or disrupt transportation services, creating privacy concerns and public backlash. Secure APIs demonstrate a commitment to protecting citizen data while ensuring the reliability of public services.

### **Innovation and Security: A Balancing Act**

APIs are the backbone of smart city initiatives, enabling interoperability between Internet of Things (IoT) devices, open data platforms, and mobile applications. However, innovation must not come at the expense of security.

A breach in a smart city's API could compromise interconnected systems — such as traffic lights, energy grids, or surveillance cameras — and thus pose serious safety risks. By prioritizing API security, local governments can embrace innovation with confidence, ensuring that new technologies remain resilient against cyber threats.

### **Financial Implications of API Breaches**

The financial toll of cyber attacks is staggering. According to [researchers at Akamai](#), the average cost of a data breach rises by 12.6% (on average \$5.05 million) when an organization is noncompliant. For local governments operating under tight budgets, such costs are unsustainable.

Proactive investment in API security is a cost-effective strategy to mitigate these risks. Secure development practices, regular vulnerability assessments, and robust monitoring tools can help local governments avoid the financial and operational fallout of breaches.

### **A Secure Path Forward**

APIs are integral to the digital ecosystems powering modern cities, counties, and regional districts. Ensuring API security is about more than protecting data — it's about safeguarding citizens, maintaining public trust, and fostering innovation.



Solutions like [Akamai API Security](#) play a crucial role in this effort by providing advanced protection against API-based threats, including bot attacks, data exfiltration, and DDoS attempts. By leveraging Akamai's intelligent threat detection and real-time monitoring, local governments can ensure their APIs remain secure while maintaining optimal performance. API Security from Akamai also uses advanced tools like API discovery to build an understanding of how many APIs are currently operating in a network.

Adopting robust security measures, such as Akamai API Security, enables local governments to transform their digital infrastructures into resilient, trustworthy, and future-ready systems. The stakes are high, but with tools like these, the benefits of a secure and innovative digital landscape far outweigh the challenges.

.....

*Brian S. Dennis is the Principal Technologist for the Public Sector at Akamai Technologies, where he provides insight and strategic guidance on cybersecurity issues that the entirety of the public sector is facing. Prior to joining Akamai, he worked with university systems building the nation's first Cybersecurity Center for Business. While in the education world, he created cybersecurity programs for the US Department of Defense and the US Department of Labor and created an accessible cyber-defense range for students and businesses.*

## Security, Compliance, or Both?

By Stephanie Gass, Senior Director of Information Security, CIS

As we look to wrap up 2024, let's review how security and compliance are fundamentally different, but complementary. Doing so will help us to plan out 2025 goals and objectives related to security and compliance.

### What is Security?

The overall objective for security is to safeguard assets. Think the CIA triad of Confidentiality, Integrity, and Availability. It's about protecting the organization and stakeholders, both internal and external. No security program is a one size fits all; it is unique to each organization.

### What Are Some Elements That Make Up Security?

- IT Infrastructure
- Network Security
- Identity and Access Management
- People

From an operational perspective, security is ongoing through continuous monitoring and maintenance to reduce risk and close gaps through physical, logical, and administrative controls. Security is not solely IT's responsibility; security is everyone's responsibility.

### What is Compliance?

Compliance is a commitment to integrity that is driven by the organization's need to:

- IT infrastructure
- Meet contractual requirements,
- Align with regulatory requirements, and
- Support the organization's policies and standards.

This often takes the form of audits, internal or external, which are ongoing to measure the security implementation within the organization.

Compliance should not be viewed as a "check the box" exercise, but rather an opportunity for continuous improvement. Then why is compliance so cumbersome? There are a few reasons, but the greatest comes from regulatory and framework overload.

As a compliance professional, you should understand what frameworks need to be implemented to meet the organization's needs and find synergy

As Sean Atkinson, CISO at the Center for Internet Security® (CIS®), likes to say, "Compliance is a byproduct of good security."

among the frameworks. While that is a great foundation, there are several other elements to the overall equation, such as scoping of systems, appropriate control management, and implementation.

### Can Both Coexist?

As Sean Atkinson, CISO at the Center for Internet Security® (CIS®), likes to say, "Compliance is a byproduct of good security."

Security and compliance are interconnected through risk management. Therefore, they should be aligned. Each can exist in your environments without connecting, but then each is operating to the beat of its own drum instead of in coordination to support the organization's goals and objectives.



# Don't change *your* **TEAM**. Change *your* **STRATEGY**.

## Automate & Accelerate CIS Benchmarks Implementation

Accelerate and eliminate weeks from your implementation cycle using the staff you already have. SteelCloud's ConfigOS software automates your systems compliance scanning and remediation efforts. It creates a secure baseline in an hour, then maintains that secure baseline indefinitely with minimal human interaction, documenting every step along the way. Best of all, ConfigOS only takes 2 minutes to install and your team can be up and hardening systems after 2 hours of training, without needing any specialized expertise.

Discover the proven strategy that helps so many organizations get and stay in effortless CIS Benchmarks compliance.

Schedule your free ConfigOS demo today.



# SteelCloud<sup>®</sup>

GET COMPLIANT. STAY COMPLIANT.

 **CIS CyberMarket<sup>®</sup>**

SteelCloud is a CIS CyberMarket Partner.

[Learn More](#)



# New Supporting Resources to Help Implement CIS Critical Security Controls Version 8.1

With the release of CIS Critical Security Controls Version 8.1 earlier in 2024, our Security Best Practices team and our volunteer community have been hard at work creating and updating our other resources in the Controls ecosystem

By Brian de Vallance, Sharon Shoemaker, and Valecia Stocchetti

Earlier this year, the Center for Internet Security® (CIS®) officially launched Version 8.1 (v8.1) of the CIS Critical Security Controls (CIS Controls), an iterative update to version 8.0. However, CIS Controls v8.1 was only the beginning of a larger refresh to the sphere of resources available to ease the implementation of our security best practices. As we've progressed through 2024, our team has been hard at work to continue to release updates to our supporting tools and resources for the CIS Controls. In the following article, we'll highlight some of the major resources we've recently released to help organizations adopt and implement our security best practices.

## A Roadmap to the CIS Critical Security Controls

The CIS Controls are a set of best practice recommendations that defend against the most common cyber attacks. The CIS Controls themselves are the framework. However, there is a broader ecosystem that surrounds the CIS Controls that offers guidance, tools, resources, mappings, and more to help facilitate the adoption and implementation of the framework.

At times, it can be overwhelming to implement any security framework. Challenges arise such as deciding what to do first, understanding what tools are available for implementation and measurement, and finding how to get help, if needed.

CIS has developed guidance to help adopters of the CIS Controls to understand what is available to them, where to start, and how to put it all together. Download our guide and see how the CIS Controls can help improve

CIS Controls v8.1 was only the beginning of a larger refresh to the sphere of resources available to ease the implementation of our security best practices. As we've progressed through 2024, our team has been hard at work to continue to release updates to our supporting tools and resources for the CIS Controls.

your cybersecurity posture: <https://www.cisecurity.org/insights/white-papers/roadmap-cis-critical-security-controls>

## Guide to Implementation Groups (IGs)

For those using or wanting to use the CIS Controls in their cybersecurity journeys, CIS has developed Implementation Groups (IGs) — divided into IG1, IG2, and IG3 — to help prioritize the implementation of the CIS Controls. Each IG identifies a set of CIS Safeguards that the enterprise should implement.

Every enterprise should begin with IG1, which is referred to as "essential cyber hygiene," as it represents a

minimum standard of information security that is the on-ramp to implementation of the CIS Controls. Once IG1 has been implemented, enterprises can move to CIS Safeguards in IG2 and IG3 based on the factors mentioned above. Keep in mind that CIS Safeguard implementation is not a one-time activity. It is an iterative approach to protecting an enterprise amidst changing environments, threats, and business objectives.

The IGs provide a simple and accessible way to help enterprises of different classes focus their efforts on a specific set of best practices that will maximize the value (i.e., protection) when it comes to defending against cyber attacks. This brings us to a question. Which IG does your enterprise leverage?

Download our guide to efficiently and less subjectively determine your IG: <https://www.cisecurity.org/insights/white-papers/guide-implementation-groups-ig-cis-critical-security-controls-v8-1>.

### **Establishing Essential Cyber Hygiene Version 8.1**

Study after study and test after test gives us the same depressing result: almost all successful attacks take advantage of conditions that could reasonably be described as "poor hygiene," including failure to patch known vulnerabilities, poor configuration management, and inefficient management of administrative privileges.

At CIS, we attribute these failures primarily to the complexity of modern systems management as well as a noisy and confusing environment of technology, marketplace claims, and oversight and regulation ("The Fog of More"). Any large-scale security improvement program thus needs a way to bring focus and attention to the most effective and fundamental things that need to be done.

We do this at CIS by defining "essential cyber hygiene" as consisting of the Safeguards found in Implementation Group 1 (IG1) of the CIS Controls. By defining IG1, we then specify tools that can be put in place to implement the actions, measurements to track progress or maturity, and reporting that can be used to manage an enterprise improvement program. This approach provides a specific way to negotiate "trust" and an "expectation" of security.

IG1 is not just another list of good things to do; it is an essential set of steps that helps all enterprises deal with the most common types of attacks we see in real life. Our new guide, *Establishing Essential Cyber Hygiene Version 8.1*, is a resource to assist with the implementation of essential cyber hygiene in alignment with the Nationwide Cybersecurity Review (NCSR) and National Institute of Standards and Technology Cybersecurity Framework

(NIST CSF) by providing needed tools, resources, and templates.

Download the guide today to get started on your cybersecurity journey: <https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene-version-8-1>.

### **Reasonable Cybersecurity Guide**

In the United States, there is no national, statutory, cross-sector minimum standard for information security. No national law defines what would be considered reasonable security in matters involving data breaches. The federal and state governments have various statutes, regulations, policies, and caselaw covering elements of cybersecurity, like data breach notification and data privacy.

But all of these efforts fail to specify what an organization must do to meet the standard of reasonable cybersecurity.

We've sought to change that. In collaboration with recognized technical cybersecurity and legal experts, CIS published practical and specific guidance to organizations seeking to develop a cybersecurity program that satisfies the general standard of reasonable cybersecurity. This guidance, in turn, could be a valuable resource to assist cybersecurity professionals, counselors, auditors, regulators, businesses, and consumers as well as lawyers and courts in assessing whether an organization's program meets this same standard when the compromise of protected information gives rise to litigation or regulatory action. An equally important goal for publishing this guidance is to reduce litigation resulting from data breaches. Building on federal and state laws, existing regulations, various industry best practices and cyber frameworks, and other resources, our guidance identifies what is minimally adequate, absent express law governing the circumstances, for information security protections commensurate with the risk and magnitude of harm that could result from a data breach.

Finally, our guidance provides how one framework, the CIS Controls, can be implemented prescriptively and in a manner that affords all those who use and rely on the technology ecosystem the ability to assess whether reasonable cybersecurity measures were taken.

To learn more, download *A Guide to Defining Reasonable Cybersecurity*: <https://www.cisecurity.org/insights/white-papers/reasonable-cybersecurity-guide>.

You can also watch a recording of our webinar, "The Rise of Reasonable Cybersecurity," to hear from some of the

guide's authors on implementing reasonable cybersecurity in your organization: <https://www.cisecurity.org/insights/webinar/rise-of-reasonable-security>.

## Guide to Asset Classes

As part of our process to evolve the CIS Controls, we establish "design principles" that guide us through any minor or major updates to the document. Our design principles for CIS Controls v8.1 are context, clarity, and consistency. Context enhances the scope and practical applicability of Safeguards by incorporating specific examples and additional explanations. Clarity aligns with other major security frameworks to the extent practical while preserving the unique features of the CIS Controls. Consistency maintains continuity for existing CIS Controls users, ensuring little to no change due to this update.

At the very foundation of the CIS Controls are a few critical actions that surround knowing your environment. When implementing and auditing the CIS Controls, there are several references to terms such as enterprise assets, software, end user devices, and more. CIS simplified the language in Version 8 to provide enterprises with guidance on how enterprise assets and software are organized in the CIS Controls and to help explain what we mean when we say things like "Establish and Maintain Detailed Enterprise Asset Inventory." In Version 8.1, the CIS restructured Asset Classes and their respective definitions to ensure consistency throughout the Controls.

Download *Guide to Asset Classes: CIS Critical Security Controls v8.1* today and learn how to make the implementation of the CIS Controls a success in your organization: <https://www.cisecurity.org/insights/white-papers/guide-to-asset-classes-cis-critical-security-controls-v8-1>.



*Brian de Vallance is a Senior Advisor at Cambridge Global Advisors. Previously, he served as the Vice President of Policy & Outreach for the Center for Internet Security (CIS). De Vallance was responsible for monitoring and coordinating CIS's contributions to cybersecurity policy at all levels of government including the U.S. Congress, the White House, and key state and local government associations. Prior to CIS, de Vallance served in a number of senior roles at the U.S. Department of Homeland Security (DHS), including Assistant Secretary for Legislative Affairs. In this position, de Vallance acted as the DHS's principal liaison with the U.S. Congress, coordinating the Department's legislative activity. Prior, he served in other roles at DHS, such as Senior Counselor to then-Secretary Janet Napolitano, Chief of Staff to then-Deputy Secretary Jane Holl Lute, and senior accountable officer for the implementation of the American Reinvestment and Recovery Act. De Vallance also previously served U.S. Attorney General Janet Reno as the U.S. Department of Justice's Director of Intergovernmental Affairs and its Federalism Officer. He graduated from Brown University and Arizona State University's College of Law.*

*Sharon Shoemaker is Executive Coordinator for the Security Best Practices team at the Center for Internet Security (CIS). Prior to CIS, Shoemaker formally held senior executive roles in the U.S. Federal Government and spent the majority of her career in cybersecurity and its predecessor disciplines.*

*Valecia Stocchetti is a Senior Cybersecurity Engineer for the Center for Internet Security (CIS). As a member of the CIS Critical Security Controls team, she has led multiple projects, including the CIS Community Defense Model (CDM) v2.0, the CIS Risk Assessment Method (CIS RAM) v2.1, as well as multiple Living off the Land (LotL) guides and the Blueprint for Ransomware Defense. Prior to joining the team, she led the Computer Incident Response Team (CIRT) at the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS-ISAC® and EI-ISAC®). While managing CIRT, Stocchetti spearheaded multiple forensic investigations and incident response engagements for the MS- and EI-ISAC's State, Local, Tribal, and Territorial (SLTT) community. Stocchetti came to CIS from the eCommerce field, where she worked complex financial fraud cases. She holds many certifications, including GIAC Certified Forensic Examiner (GCFE), GIAC Certified Forensic Analyst (GCFA), and GIAC Security Essentials Certification (GSEC). Stocchetti earned a bachelor's degree in Digital Forensics at the University of Albany, State University of New York and a master's degree in Information Security from Champlain College.*



**CIS Hardened Images<sup>®</sup>**

# Work more securely in the cloud

**Microsoft Windows 10 and 11  
in Azure Marketplace**

**LAUNCH NOW**

**CIS<sup>®</sup>**

## Wrapping Up Another Successful Year of Helping Our Members Get the Most Out of Their Membership

By Kelly Morris, Director of Maturity Services, MS-ISAC

As we round out another year of providing dedicated support to U.S. State, Local, Tribal, and Territorial (SLTT) members of the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), we wanted to share a look back at everything our members have accomplished this year.

Leading the charge from the Center for Internet Security® (CIS®) is our very own Stakeholder Engagement team, which is laser-focused on helping MS-ISAC members get the most out of their membership and improve their cyber maturity.

The Stakeholder Engagement team continues to conduct outreach and foster strong relationships with MS-ISAC members and key stakeholders.

Throughout 2024, the team successfully planned and implemented five (5) regional events delivering on growth and awareness of ISAC services and developing relationships to further expand our reach and increase adoption of CIS Services®. These events also provided networking and collaboration opportunities among members, while also giving CIS the opportunity to share information into the resources available to them as members.

Let's take a look at these events together.

### Arizona Cyber Partners

*Scottsdale, Arizona | April 2024*

Over 100 attendees from various SLTT government organizations in the State of Arizona came together for a full-day event hosted by the MS-ISAC, CISA, and the State of Arizona. This event was a direct response to the identified need for community, collaboration, and networking. This event provided the opportunity to learn from subject matter experts and colleagues related to challenges many of our members are facing. A day full of sessions covered topics such as:

- Elections security and the top threats facing our elections integrity
- No-cost and low-cost offerings from the MS-ISAC, CISA, and the State of Arizona
- Understanding and utilizing the CIS Critical Security Controls (CIS Controls)
- Incident response planning

With a goal of enhancing the sense of community within the State of Arizona, we did just that. Members left

the day knowing they were not alone in their cybersecurity journey and that the MS-ISAC, alongside CISA and the State, is here to help ease the difficulty of securing their organization.

### Washington K-Gray Secure by Design Conference

*Spokane, Washington | May 2024*

Over 90 attendees represented the States of Washington, Idaho, and Oregon. Washington K-Gray Secure by Design Conference provided opportunities to network with EdTech peers and learn about all the no-cost MS-ISAC and DHS-funded resources. Presentations and panel discussions included:

- Essential cyber hygiene best practices
- K-12 security trends
- Artificial intelligence
- Lessons learned from a breach
- Incident response resources
- Safe online practices and securing social media

This event moved us closer to achieving several goals:



- Build on shared mission goals with CISA Region 10.
- Strengthen CIS/MS-ISAC presence in Eastern Washington and Northern Idaho, specifically among K-12 organizations, educational service districts (ESDs), and public higher education organizations.
- Increase membership and MS-ISAC and CIS service adoption.
- Get much-needed cybersecurity and incident response resources into the hands of cyber-underserved K-12 organizations.

### Secure Our Alaska Conference

#### *Anchorage, Alaska | June 2024*

Over 200 attendees from State, Local, Tribal, and critical infrastructure organizations in Alaska attended the Secure Our Alaska Conference. Secure Our Alaska allowed for valuable networking opportunities and presentations that emphasized best practices and no- and low-cost services to improve cyber and incident response preparedness.

Building on the shared mission goals we have with CISA Region 10 and State of Alaska, and following 2023's success, we attained a 30% increase in attendance over last year's event. We strengthened our presence among cyber-underserved Local and Tribal organizations; got much-needed cybersecurity resources related to CIS Controls Implementation Group 1 (IG1), which is synonymous with essential cyber hygiene, into the hands of these underserved stakeholders; and increased MS-ISAC

membership and service adoption.

### Arkansas Regional Event

#### *North Little Rock, Arkansas | October 2024*

This event was organized in conjunction with officials from the State of Arkansas, the Arkansas Association of Counties, and the Arkansas Municipal League. Bringing together state officials, CISA representatives, and IT and cybersecurity personnel from various sectors to discuss the latest challenges and solutions in the ever-evolving world of cybersecurity, this event was focused on regional cooperation and innovation.

This two-day hybrid event saw nearly 100 attendees join either in-person or virtually. Among them were participants from state agencies such as the Arkansas Game and Fish commission, K-12 organizations, and local government. The Arkansas Regional Event provided a vital platform and opportunity for advancing cybersecurity knowledge and fostering greater resilience among SLTTs within the State of Arkansas. Attendees left with practical strategies and a sense of urgency in addressing the growing cybersecurity challenges that affect organizations and individuals alike.

### Michigan Regional Event

#### *Lansing, Michigan | November 2024*

The event was organized with partners from the State of Michigan Department of Technology,



Photo credit: Mo Charnot (Santa Fe Reporter)

Management, and Budget (DTMB); Michigan State Police (MC3); Oakland County; and Peckham Inc., which hosted the event. This event provided a networking opportunity and collaborative environment for SLTTs while increasing their cyber posture and exposing them to both no-cost and low-cost services. The overall theme of the day was incident prevention and response, with two sets of panel discussions designed for maximum discussion and audience participation. The morning panel focused on security incident prevention with a discussion around best practices to prevent an attack, while the afternoon panel focused on incident response, discussing how to prepare your incident response plan and what to do during an incident. The day also consisted of roundtable sessions on prevention and response geared towards group discussions and an opportunity to collaborate among members about suggested topics.

### Other Initiatives

Other initiatives the team has worked on to continue to foster strong relationships with MS-ISAC members and key stakeholders include:

### ***White House Office of the National Cyber Director (ONCD)***

ONCD has launched an initiative to help K-12 schools understand the resources available to help them combat emerging cyber threats. ONCD has identified protective domain name system (PDNS) services as common solutions that all schools and districts should utilize.

The MS-ISAC calls its PDNS service Malicious Domain Blocking and Reporting (MDBR).

The Stakeholder Engagement team collaborates with ONCD to establish one-day, in-person events with K-12 districts in various states. With the goal to expand the enrollment of the MDBR program, expand the MS-ISAC as a trusted resource for states and their school districts, and foster collaboration with CISA and ONCD while working to improve the cybersecurity posture and awareness of K-12 across the nation. These events have been completed in Wisconsin, New Mexico, Michigan, and Pennsylvania, with future plans to hold events in Rhode Island, Wisconsin, Virginia, Georgia, Mississippi, and New York.

### ***National Center for State Courts (NCSC)***

NCSC received an initiative grant through the State Justice Institute to conduct a series of cybersecurity workshops that will include all state courts. NCSC's goal is to help courts and their teams make progress on their cybersecurity and disaster recover preparedness. Stakeholder Engagement is contributing to that goal by providing SMEs and presentations around the CIS Controls IG1, cyber self-assessments, no-cost services, judicial threat landscape, and table-top exercises (TTXs). We have completed an online and in-person workshop in the State of Idaho, with three more being planned around the United States in 2025.

NCSC and its attendees have expressed positive feedback about our involvement and contributions. The following are just some of the comments we received:

- "You guys killed it!"
- "Excellent information."
- "The polling questions were awesome."

### ***MS-ISAC Onboarding Consultation Calls***

The Stakeholder Engagement team launched a new method to help guide new members through the onboarding process. New members get the opportunity to schedule MS-ISAC Onboarding Consultation Calls with a member of

the Stakeholder Engagement team. These are 45-minute calls providing new members with the opportunity to connect while helping guide them to sign up for services they are interested in implementing in their respective organizations. These calls are designed to help make those first few steps of joining membership easier to implement. We have simplified our messaging providing easy steps and guidance to get started.

We have received valuable feedback from members, and these calls are helping to introduce us without overwhelming the members. The following are comments we have received from members.

- "The call offered a lot of good information and educated me on the available services and how to utilize them."
- "Chance to ask questions and get a little more information on services that are useful to us vs. trying to navigate on our own."
- "I was lost as to where to start, and the rep was very helpful."

### **Conclusion**

CIS, MS-ISAC, and the Stakeholder Engagement team look forward to continuing to provide valuable resources, collaboration opportunities, and cybersecurity resources to SLTT organizations who need it most.



# Upcoming Events

## January

### January 8 - 10

The National Association of Election Officials will host their **Annual Joint Election Officials Liaison Conference (JEOLC)** at the Ritz-Carlton, Pentagon City in Arlington, VA. The event will bring together the nation's election professionals to network with peers, discuss policy considerations and legislative efforts, and hear from partner organizations. VP of the EI-ISAC Marci Andino will be a featured panelist at the event, discussing lessons learned from the 2024 general election. Learn more at <https://www.electioncenter.org/>.

### January 24

The **Sixth Annual Tampa Cybersecurity Summit** will take place at the Hilton Tampa Downtown in Tampa, FL. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/tampa25/>.

### January 27 - 30

The Idaho Association of Counties (IAC) will host the **2025 IAC Midwinter Legislative Conference** at the Boise Center in Boise, ID. The event is the premier opportunity for county officials and staff to connect with legislators, state leaders, and peers from across Idaho. As the first conference following the general election, it's the perfect time for state and local officials to engage, share fresh perspectives, and build valuable relationships. Learn more at <https://idcounties.regfox.com/2025-iac-midwinter-conference>.

### January 29 - February 1

The National Association of Secretaries of State (NASS) will host the **2025 NASS Winter Conference** at the Grand Hyatt Washington D.C. The event will bring together the nation's secretaries of state and their staff to discuss crucial industry topics, network with peers, and learn techniques and strategies to better serve their constituencies. Learn more at <https://www.nass.org/events/nass-2025-winter-conference>.

### January 31

The **12<sup>th</sup> Edition of the Atlanta Cybersecurity Summit** will take place at the Grant Hyatt Atlanta in Buckhead in Atlanta, GA. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/atlanta25-jan/>.

## February

### February 1 - 5

The Texas Computer Education Association (TCEA) will host its annual member conference, **TCEA 2025**, at the Austin Convention Center in Austin, TX. The industry-leading professional development event will bring educators — from teachers to administrators and everyone in between — from across the state together for a week of growth, connection, and discovery. Attendees will dive into the world of educational technology with illuminating sessions, opportunities for collaboration, and a full week of celebrating educators. Learn more at <https://convention.tcea.org/>.

### February 2 - 4

The National Association of State Election Directors (NASED) will host the **2025 NASED Winter Conference** in Washington, D.C. The event will bring together state election officials and their staff to debrief and discuss lessons learned from the 2024 elections, connect with peers, and learn best practices and strategies to continue promoting accessible, accurate, and transparent elections. Learn more at <https://www.nased.org/-conferences>.

### February 5 - 7

The Idaho Education Technology Association (IETA) and the Organization for Educational Technology and Curriculum (OETC) will host IETA's annual member conference, **IETA 2025**, at the Boise Center in Boise, ID. The event will bring together education technology leaders and professionals from across the state to learn from industry experts, engage and network with peers, and discover innovative solutions to improve the learning environment for their schools, teachers, and students. Learn more at <https://ieta.events/>.

### February 12

The **Ninth Edition of the Silicon Valley Cybersecurity Summit** will take place at the Santa Clara Marriott in Santa Clara, CA. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/siliconvalley25-feb/>.

## February 19

The **Seventh Edition of the Philadelphia Cybersecurity Summit** will take place at the Philadelphia Marriott Downtown in Philadelphia, PA. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/philadelphia25-feb/>.

## February 19 - 21

**Right of Boom** will take place at the MGM Grand Resort in Las Vegas, NV. Right of Boom is the only vendor agnostic cybersecurity conference dedicated to improving the cyber maturity and success of MSP/MSSPs. The conference will bring together MSP/MSSPs leaders and stakeholders to learn from industry experts, network with peers, and share their knowledge. CIS Executive VP of Security Best Practice Curtis Dukes and VP of Security Best Practice Content Development Phyllis Lee will be featured speakers at the event. Learn more at <https://www.rightofboom.com/rob-2025>.

## February 20

The **Fifth Edition of the San Diego Cybersecurity Summit** will take place at the Marriott Marquis San Diego Marina in San Diego, CA. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/sandiego25-feb/>.

## February 26 - 28

TribalHub will host the **5<sup>th</sup> Annual TribalHub Cybersecurity Conference** at Miccosukee Casino and Resort in Miami, FL. Being held in person for the first time, the conference will bring together tribal IT leaders and professionals from across the country to learn from industry experts, share their experiences and best practices, and connect with their peers. Learn more at <https://www.tribalhub.com/tribal-cybersecurity-summit/>.

## February 27

CrowdStrike will host **Fal.Con Gov** at the Ronald Reagan Building and International Trade Center in Washington, D.C. The event will bring together nearly 1,000 cybersecurity leaders alongside government thought leaders, industry experts, and CrowdStrike executives for a transformative day of insights, innovation, and connection. Learn more at <https://www.crowdstrike.com/events/fal-con-gov/>.

## March

### March 1 - 4

The National Association of Counties (NACo) will host the **2025 NACo Legislative Conference** at the Washington Hilton in Washington, D.C. The event will bring together nearly 2,000 county officials from across the nation to focus on federal policy issues that impact counties and their residents. Attendees will engage in policy sessions, interact with officials of the new administration, and meet with members of Congress to strengthen intergovernmental partnerships for years to come. Learn more at <https://www.naco.org/event/2025-naco-legislative-conference>.

## March 3 - 6

**SXSW EDU Conference and Festival** will take place at the Austin Convention Center in Austin, TX. The conference is a vibrant and dynamic event that brings together the brightest minds in education to tackle complex issues and drive impact to create a new tomorrow for learners everywhere. CIS VP of Security Operations and Intelligence Randy Rose will be a featured panelist at the event. Learn more at <https://www.sxswedu.com/>.

## March 3 - 6

The Healthcare Information and Management Systems Society (HIMSS) will host the **HIMSS Global Health Conference and Exposition** at the Venetian Convention and Expo Center in Las Vegas, NV. This premier event for the healthcare industry will bring together health IT and cybersecurity leaders and professionals from around the world seeking to stay ahead of industry trends, connect with like-minded professionals, and explore cutting-edge solutions transforming healthcare. Attendees will forge connections within a community of healthcare experts from across the digital health ecosystem, immerse themselves in captivating sessions led by sought-after speakers, and learn about crucial topics to help advance their careers. Learn more at <https://www.himssconference.com/>.

## March 5

The **Ninth Annual Denver Cybersecurity Summit** will take place at the Hilton Denver City Center in Denver, CO. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/denver25/>.

## March 6

The **15<sup>th</sup> Edition of the New York Cybersecurity Summit** will take place at the Sheraton New York Times Square Hotel in New York, NY. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/newyork25-march/>.

## March 10 - 12

The National League of Cities (NLC) will host its **Congressional City Conference** at the Marriott Marquis Washington, D.C. The conference is where the local leaders' voices take center stage on Capitol Hill and provides them the unique chance to engage on federal policy and build partnerships critical to the future of their local government. Leaders from municipalities across the country will connect with federal officials; learn about funding opportunities available to cities, towns, and villages; and add their voices to NLC's federal municipal policy. Learn more at <https://ccc.nlc.org/>.

## March 11 - 12

Billington Cybersecurity will host its **2<sup>nd</sup> Annual Billington State and Local Cybersecurity Summit** at the Ronald Reagan Building & International Trade Center in Washington, D.C. The conference will bring together top federal, state, local, and tribal government officials along with industry experts to share best practices, learn from one another, enhance current cyber operations and bolster future defenses. A number of SMEs from CIS and the MS- and EI-ISACs will be featured speakers at the event. Learn more at <https://statelocal.billingtoncybersummit.com/>.

## March 13

The **Ninth Edition of the Seattle/Bellevue Cybersecurity Summit** will take place at the Hyatt Regency Bellevue in Bellevue, WA. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/seattle25-march/>.

## March 24 - 25

Zscaler will host its **2025 Public Sector Summit** at the Ronald Reagan Building & International Trade Center in Washington, D.C. Attendees of the conference will learn next steps on their IT modernization journey and on their efforts to embrace innovation. They'll hear from prominent government IT leaders and industry experts who will provide valuable use cases and actionable insights for each stage of the transformation journey — from initial assessments and strategy building to implementation and ongoing optimization. Learn more at <https://reg.rainfocus.com/flow/zscaler/pss25/LandingPage/page/LandingPage>.

## March 27

The **Fifth Annual South Florida Cybersecurity Summit** will take place at the Diplomat Beach Resort in Hollywood, FL. It will bring together leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, U.S. SLTT government entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/southflorida25/>.

## March 31 - April 2

The Consortium for School Networking (CoSN) will host its annual membership conference, **CoSN 2025**, at the Hyatt Regency Seattle in Seattle, WA. The event will allow attendees to learn about the hottest topics in EdTech. They'll join peers from around the country to network, learn, share, and discuss crucial issues affecting school districts, such as cybersecurity, digital equity — and the topic that's on everyone's mind: artificial intelligence. Learn more at <https://www.cosn.org/cosn2025/>.



## Interested in being a contributor?

---

### Please contact us:

[cybermarket@cisecurity.org](mailto:cybermarket@cisecurity.org)

[www.cisecurity.org](http://www.cisecurity.org)

518.266.3460

-  [cisecurity.org](http://cisecurity.org)
-  [info@cisecurity.org](mailto:info@cisecurity.org)
-  518-266-3460
-  Center for Internet Security
-  @CISecurity
-  TheCISecurity
-  cisecurity
-  CenterforIntSec