Testimony of Scott C. Algeier

Executive Director, Information Technology-Information Sharing and Analysis Center

To the House Committee on Homeland Security

Subcommittee on Cyber Security and Critical Infrastructure Protection

"Data Centers, Telecommunications Networks, and Space-Based Systems: Modernizing DHS's Role for the Communications and IT Sectors"

April 29, 2026

Chairman Ogles and Members of the Committee,

Thank you very much for the opportunity to testify today. My name is Scott Algeier and I have spent over twenty-five years at the intersection of cybersecurity policy and operations. I am the Founder, President, and CEO of cybersecurity consulting firm Conrad, Inc., Executive Director of the Information Technology – Information Sharing and Analysis Center (IT-ISAC), and Executive Director of the Food and Agriculture – Information Sharing and Analysis Center.

I am also a member of the Executive Committee of the IT Sector Coordinating Council and past Vice Chair of the National Council of ISACs. I previously served as Executive Director of the Industry Consortium for Advancement of Security of the Internet (ICASI), and as Manager for Homeland Security at the U.S. Chamber of Commerce.

It is an honor to be here today.

About the IT-ISAC

Founded in 2000, the mission of the Information Technology-Information Sharing and Analysis Center (IT-ISAC) is to grow a diverse community of companies that leverage information technology and have in common a commitment to cybersecurity. We serve as a force-multiplier that enables collaboration and sharing of relevant, actionable cyber threat information, effective security policies, and practices for the benefit of all.

The premise of the IT-ISAC is simple—we're stronger together. At a time when well-resourced and highly-skilled nation-state actors are targeting industry, the IT-ISAC provides a forum for companies to share threat intelligence, increase situational awareness, and identify appropriate mitigations. We help companies make informed risk management decisions.

Our membership base spans almost every segment of the IT sector, including data centers, cloud and Critical SaaS providers, semiconductor manufacturers, hardware and software companies, AI, and other technologies that propel the global economy. Members regularly exchange threat intelligence, discuss common security challenges, analyze threats, and share effective practices and have access to the following benefits:

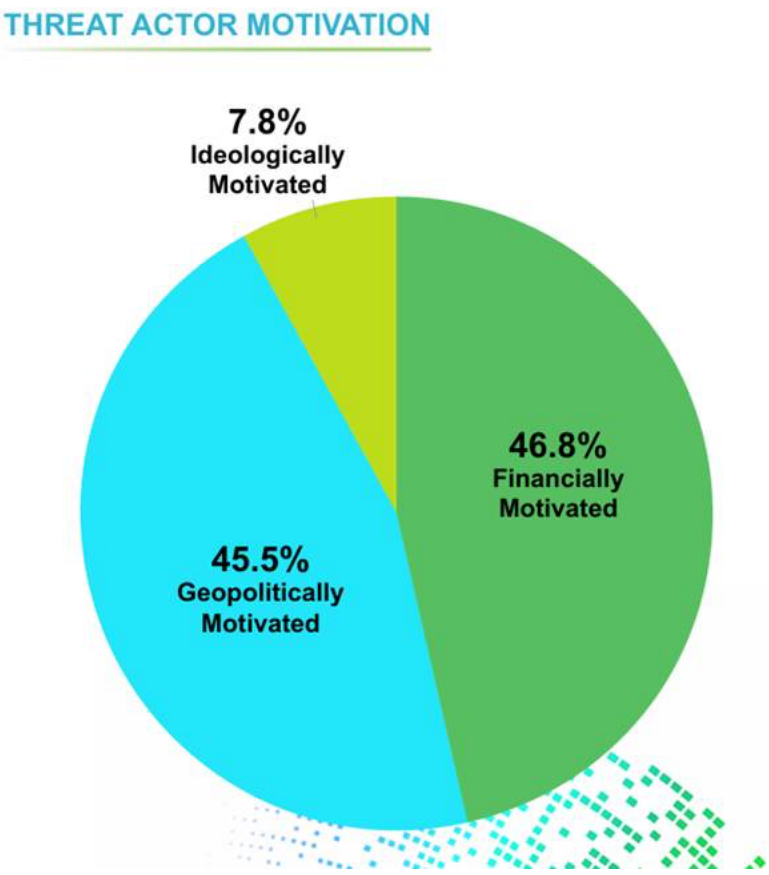
- Access to 330+ Adversary Attack Playbooks mapped to the MITRE ATT&CK® Framework, enabling members to share and learn tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs).
- Ransomware Tracker that contains 15,000+ reported ransomware incidents, including those specific to the IT and food and agriculture sectors.
- A Threat Intelligence Platform with access to industry-leading threat analysis and automated indicator sharing.
- Daily Threat Reports, weekly newsletters, and incident-specific reporting as needed, offering timely analysis to assist with informed risk management.
- Special Interest Groups (SIGs), facilitating discussion among members on security topics and industry segments.

The IT-ISAC is governed by a board of directors composed of dues-paying member companies and does not receive any funding from any government entity.

Cyber Threat Environment

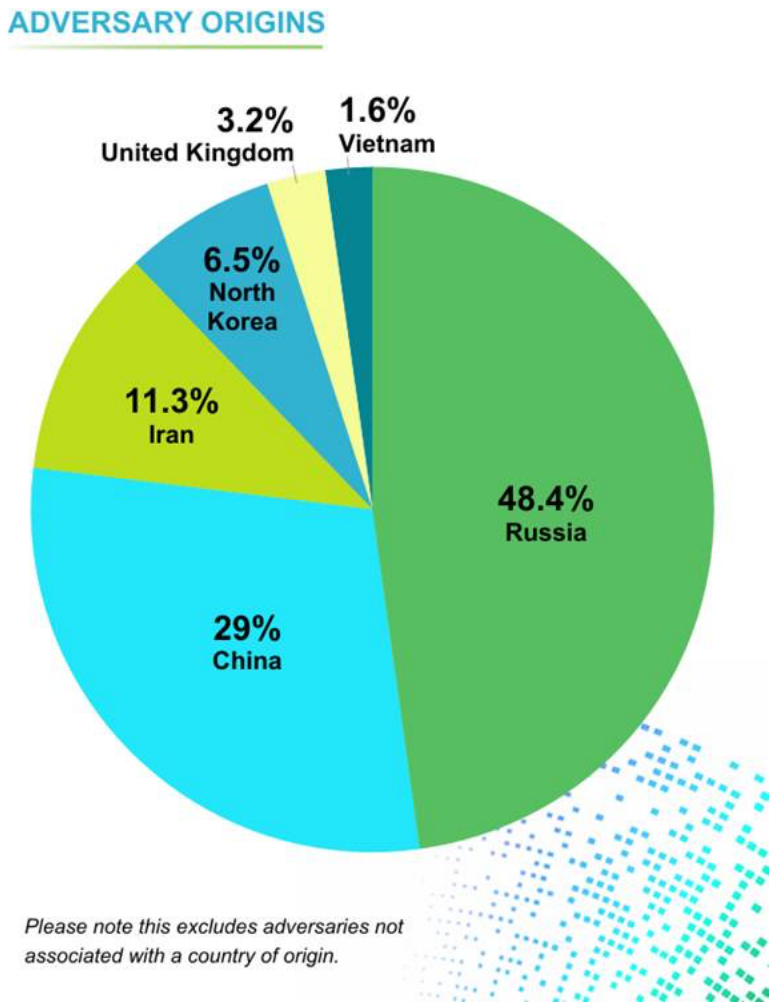
The country faces an unprecedented array of cyber risks. Networks are interconnected across the globe. The pace of technological change is exploding. Corporate budgets are constrained. Threat actors are collaborative, highly skilled, and well-financed. In fact, the economics favor the attackers. It is much more expensive to defend than it is to attack.

The IT-ISAC's 2025 IT Sector Cyber Threat Report available at https://www.it-isac.org/resources reveals some interesting trends. About 45% of the actors we observed in 2025 were nation-state actors. About 8% were ideologically motivated, generally (but not always) aligned with nation-state actors. The remaining 47% were ransomware operators or other cyber criminal gangs seeking financial gain. These are percentages of observed threat actors, and not percentages of observed attacks.



Actors based in China account for 29% of the actors we observed. China strives for long-term persistence. They are known to hide on networks for months or even a year or more before being detected. We must assume that China-based actors have undetected access to critical government and private sector networks and be prepared for the possibility that they intend to use this access to cause disruptions or damage.

Over 48% of all threat actors we observed in 2025 were based in Russia. Russia is teeming with talented nation-state actors and cyber criminals. Russia has also demonstrated its capability and intent to launch disruptive attacks against critical infrastructure across the globe. In addition, we are seeing signs that Russian affiliated actors have aligned with Iranian actors, amplifying Iranian affiliated attacks and targeting companies in solidarity with Iran.



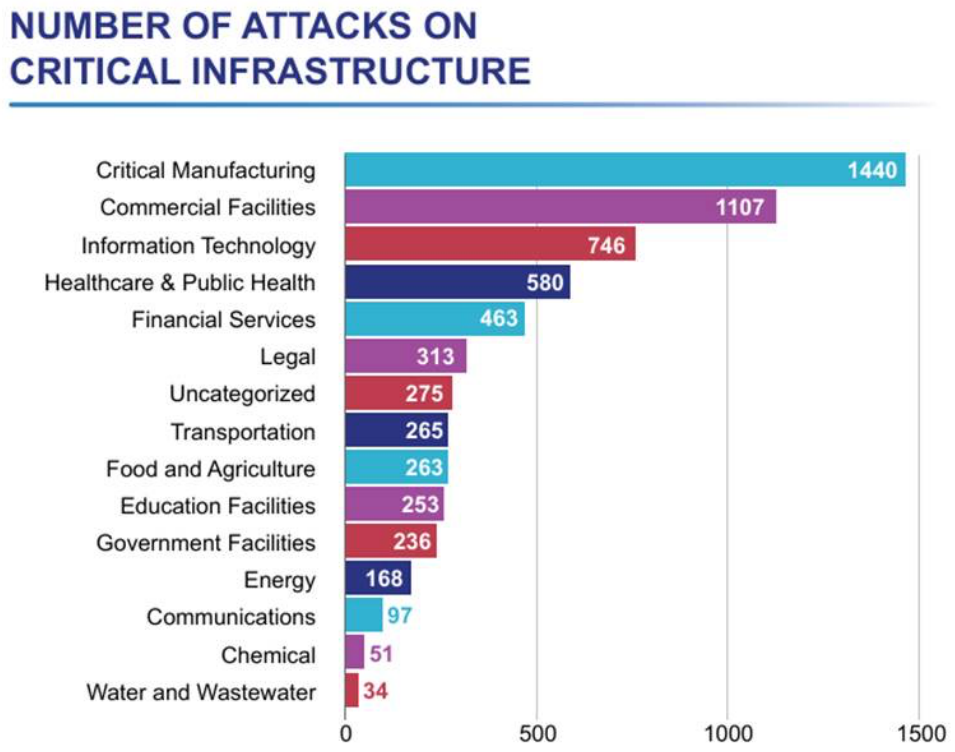
Iran is highly capable in the cyber domain. About 11% of observed threat actors active in the sector are based in Iran. Although the line between a nation-state actor and an affiliate actor can be blurry, Iran hosts a range of actors who operate with the blessing of the Iranian authorities. These threat actors have previously attacked critical infrastructure companies

across the Middle East and within the United States. Iranian aligned actors are continuing their attacks during the current conflict.

Finally, in terms of nation-states, 6.5% of observed actors are based in North Korea. North Korea deploys highly skilled actors to both steal sensitive information as well to fund their military. The now famous Democratic People's Republic of Korea (DPRK) fake worker scams are highly organized, well implemented, and provide millions of much needed dollars to fund their government. Despite increased attention these attacks are receiving, they continue to be successful.

Beyond nation-state actors, ransomware actors continue to target companies across the critical infrastructure sectors. While most Ransomware actors are not affiliated with nation-states, some nation-state actors do deploy ransomware. We are also seeing nation-state actors collaborate with ransomware operators.

The IT-ISAC's recently released Annual Ransomware Report (https://www.it-isac.org/resources), is based on 6,351 ransomware incidents we tracked in 2025. Of these, 746 attacks were observed in the IT sector, accounting for 11.8% of the total. This is a sharp increase from the 3,562 incidents we tracked in 2024 (over 78% growth), 300 of which were observed in the IT sector.



Observed number of attacks on critical infrastructure from the IT-ISAC 2025 Ransomware Report.

It must also be noted that artificial intelligence (AI) is making the attackers not only more efficient but also better. Threat actors use AI to improve the quality, quantity, and scale of their attacks. With the use of AI, attacks that took humans multiple days to complete can now be conducted within hours. While AI is being used for network defense, the advantage is with the attackers, at least for the moment. The capabilities announced by Anthropic of its Claude Mythos model risks breaking the traditional models that govern coordinated vulnerability disclosure and patch management. These models operate at the scale and speed of humans, not at the scale of AI.

Collaborating with CISA

The IT-ISAC and CISA share the common mission of defending against today's threats while planning for the risks of the future. The IT-ISAC has long partnered with CISA on a range of operational, policy, and planning initiatives. We are committed to helping CISA succeed because when CISA succeeds, the country succeeds.

As part of our commitment, we are part of the Joint Cyber Defense Collaborative (JCDC). While we find the Known Exploited Vulnerability Catalog to be helpful and appreciate the indicators and alerts we receive from the JCDC, overall, the JCDC represents a missed opportunity. One key potential value of the JCDC is to collaborate across sectors. The JCDC is actively sharing across sectors, but we have not been part of any cross-sector collaborations through the JCDC.

In contrast, the private sector continues to demonstrate how cross industry collaboration drives value. The IT-ISAC worked with nine other members of the National Council of ISACs, including the Space ISAC, to release a public advisory on threats posed by Iranian threat actors. The feedback on it was overwhelmingly positive. While we appreciate this, our advisory incorporated only open-source intelligence and is something CISA could have easily developed or coordinated.

Improving analytic collaboration is essential. There is a great need for an integrated capability that provides industry and government common situational awareness, one that enables CISA and industry to jointly identify, analyze, and mitigate threats. In the past, this has been referred to as a "Cyber Weather Map." Previous efforts to build this capability had faltered, and it was claimed that JCDC would serve this purpose. However, the JCDC was built largely without broad industry engagement, so it is not surprising that the JCDC has not achieved this capability.

The IT-ISAC continues to welcome the opportunity to share threat intelligence with CISA and collaborate on the development of analytic products. Our desire is to provide CISA analysts with an understanding of the trends, actors, and TTPs we are observing and compare those with what CISA is seeing. This will provide focus to our sharing—instead of throwing indicators at each other, we can curate indicators related to specific threats or information needs.

Renewing the Cyber Information Sharing Act of 2015 (CISA 2015) is critical to enabling this. Renewal will sustain threat intelligence sharing and operational collaboration. Industry has come to depend on the legal certainty CISA 2015 provides and has established internal sharing policies based on it. Losing these protections will create uncertainty and be needlessly disruptive. It could disrupt the flow of threat intelligence industry shares with each other, and almost certainly will reduce what is shared with CISA. Who wants to voluntarily share sensitive security information with the government if it is subject to Freedom of Information Act requests? At a time when industry and government both are under sustained attack, government policy should be to encourage the voluntary sharing of cyber threat intelligence.

The IT-ISAC has a strong relationship with CISA's Stakeholder Engagement team. The team had been helpful in connecting us with various elements within CISA to drive further engagement. We met with the Stakeholder Engagement team no less than once per month, and they were always responsive whenever we needed them. Unfortunately, as a result of the shutdown, these calls were suspended.

Recognizing this, however, there is much more engagement with the Stakeholder Engagement team can accomplish more. There are serious security challenges that need to be addressed, new risks that need to be understood and mitigated, and contingencies that need to be planned for. This work is normally done through the Stakeholder Engagement team under the CIPAC framework. However, in February 2025 CISA paused its engagement with industry, then DHS disbanded CIPAC in March 2025, suspending all working groups and projects between industry and CISA.

For over a year, we have been hearing that CISA will reinstate the protections of the CIPAC framework through a new council. This is encouraging. However, industry has not been consulted on the development of this new council and we have few details on it. Further, there are questions as to whether CISA maintains the capacity to adequately manage and support the work of the new council once it is activated.

In addition, the ongoing shutdown is impacting engagement with CISA, in areas that do not require CIPAC protections. As one example, CISA was working to understand interdependencies related to data centers and wanted to meet with our Data Center Special Interest Group. However, these meetings have not taken place since the CISA team doing the work was furloughed during the shutdowns.

Improving the CISA Partnership

One of our biggest challenges in cybersecurity is resources. There simply are not enough people, time, or money to do what needs to be done. We therefore must allocate our limited resources to maximum effect. An effective partnership will enable industry and government to make informed decisions on how to allocate those resources.

However, too often the government's concept of partnership is that it makes the policy and industry implements it. Instead of discussing a problem together to identify solutions, the government model too often is to propose a solution itself and offer industry a short timeframe to provide feedback. The government also determines what feedback it will incorporate. When the product is released, the government promotes its "engagement" with industry. This does build trust or lead to good security outcomes,

It does not have to be this way. In 2012, the IT Sector Coordinating Council conducted a study to identify what makes a partnership successful. It examined various initiatives that succeeded, and various initiatives that did not. This work identified 12 practices that were common among successful outcomes. I no longer have access to the original report, but Larry Clinton at the Internet Security Alliance captured these practices in an article that appeared in the Journal of Strategic Security[1] in 2015.

When the report was released, these practices were widely endorsed. DHS committed to formally incorporating them into their management of the partnership. They also expressed their intent to have other Sector Specific Agencies (now known as Risk Management Agencies) adopt them. Ultimately, that commitment was not implemented, and these lessons have largely been forgotten. But at a time when CISA is looking to reset its engagement with industry, CISA should review and adopt these practices as their guideposts for engaging with industry.

The report identified the following practices:

- Senior level commitment to the partnership process communicated to staff and upper echelons.
- Involvement at the priority/goal and objective phases of projects, not just implementation.
- Use of the process identified in the NIPP ([National Infrastructure Protection Plan)] for involving industry.
- Reaching out to stakeholders early on, ideally at the "blank page" stage.
- Continuous and regular interaction between government and industry stakeholders.
- Providing adequate time for stakeholder review (equivalent to government review).
- Establishing co-leadership of programs.
- Consensus partnership decision making.
- Communicating genuine interest in stakeholder input e.g. via co-drafting.
- Adequate engagement from federal agencies beyond DHS.
- Government follow through on partnership related decisions.
- Adequate and competent support services (Clinton, 2015).

[1] Larry Clinton, "Best Practices for Operating Government-Industry Partnerships in Cyber Security," *Journal of Strategic Security* 8, no. 4 (Winter 2015): 53–68, https://www.jstor.org/stable/26465215.

A key lesson from this is that the process impacts the outcome. If the process is designed to receive broad input, identify consensus, and engage industry and government as equals, it will likely succeed. If industry believes their input matters and is taken seriously, they will engage. If they believe the outcome is predetermined and that their input does not matter, they will not.

Strengthening CISA

The good news is that there is a path to renew and strengthen CISA. This could be achieved through the following actions:

- **Implement a Replacement for CIPAC**. On March 7, 2025 CISA disbanded the CIPAC, removing the legal framework that enabled and protected strategic engagement between CISA and industry. As a result, most work with CISA is at a standstill. The Sector Coordinating Councils have not met with their Sector Risk Management Agencies in over a year. Meanwhile, our adversaries have not paused or stopped. They are attacking with impunity.
- **Provide for a Long-Term Extension of the Cybersecurity Information Sharing Act of 2015 (CISA 2015)**. CISA 2015 is a critical tool, as it provides liability and anti-trust protections for sharing cyber threat intelligence within industry. It also provides FOIA protections to cyber threat information voluntarily shared with the government. It is important to maintain a trusted legal framework that incentivizes and protects companies who voluntarily share threat intelligence.
- **Confirm a CISA Director.** While this is not the purview of the House, it is worth noting that the nominee for CISA Director recently withdrew from consideration after having his nomination languish for over a year. The absence of a Senate confirmed Director creates a leadership gap and makes it harder to advocate for resources and priorities. While Nick Andersen is doing an admirable job as Acting Director, the agency will benefit from having a Senate confirmed Director.
- **Prioritize Resources Through Collaboration**. The list of things we want to do to improve our collective security is infinite. The list of things we can do is finite. Resources—time, money and people-- are limited and must be leveraged to maximum effect. Collaboratively developing priorities can help industry and government allocate resources more effectively.
- **Analyze the Impacts of CISA Staff and Funding Reductions**. Changing staffing levels based on organizational priorities is a common management practice. However, the size of the CISA reductions have caused many to wonder whether CISA can maintain its vital core functions. CISA should engage with its partners to understand what impact the reductions are having and evaluate whether any adjustments are warranted.
- **Enhance Analytic Engagement with Industry**. CISA can improve its engagement with the critical infrastructure sectors by designating specific cybersecurity analysts to support specific sectors. These analysts would build relationships with sector ISACs and their members to know and understand their industries, share threat intelligence specific to that sector, and receive threat intelligence and requests for information shared by industry. They would be an analytic point of contact for specific sectors.

Under this concept, one analyst could support multiple sectors (for example, one analyst could cover IT, Communications, and Space).

- **Create Common Situational Awareness.** The JCDC currently engages with industry by sending alerts on specific incidents through Slack. On occasion, they will stand up working groups to address specific issues. But this "whack a mole" approach is not a substitute for a sustained capability that shares, in near real time, strategic and tactical threat intelligence that informs decision making. One potential goal could be to build a threat intelligence dashboard that is accessible to the industry and government.
- **Vulnerability Management Modernization**. Our vulnerability and patch management processes are already struggling to keep up with today's pace of disclosures. At the same time, the time between the disclosure of a vulnerability and its exploitation has decreased from weeks and days to hours. Threat actors are exploiting vulnerabilities before organizations can deploy patches. AI threatens to further stress, if not disrupt, our vulnerability disclosure and patch management models. CISA can play an important role in convening the relevant communities to address this.
- **Refining Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).** CIRCIA was passed in 2022 with draft regulations being proposed by DHS in April 2024. The IT-ISAC and the IT Sector Coordinating Council expressed concern that the proposed regulations were too broad and would result in CISA receiving more information than it could process. Limiting CIRCIA's scope and scale to more closely align with legislative intent will not only reduce the reporting burden on industry but will help CISA develop and distribute more meaningful threat intelligence. We applaud CISA for planning a series of town halls to receive additional input.
- **Implement Effective Partnership Principles.** Managing a partnership takes work. In 2012 the IT Sector Coordinating Council conducted a study that identified 12 practices that, if followed, lead to successful outcomes. These have largely been forgotten, but at a time when CISA is looking to reset its engagement with industry, CISA should adopt these practices as their guideposts for engaging with industry.

Conclusion

The IT-ISAC has been partnering with the government for 26 years. We value our partnership with CISA and are committed to and vested in its success. There is no doubt that CISA is facing some headwinds, but through these headwinds are opportunities. We appreciate the work we do with CISA and are determined to do what we can to help it succeed.

We look forward to continuing our work with CISA and others across government to ensure the digital infrastructure that propels the global economy is secure and resilient. Please feel free to contact me at salgeier@it-isac.org if you have any questions or if I can be of any assistance.

Thank you again for the opportunity.