Mr Chairman, Ranking Member, and Members of the Subcommittee on Cybersecurity and Infrastructure Protection, thank you for the opportunity to testify before your subcommittee and share with you my thoughts on the protection of the swiftly evolving telecommunications, information technology, and space ecosystems, all of which are vital to our national and economic security.

I have the honor to serve as the Chair of the Board of Directors of the Space Information Sharing and Analysis Center, or Space ISAC. Founded in 2019, the Space ISAC is the principal information sharing platform for industry – and between industry and government – regarding threats to our space systems. While our initial focus was on cyber threats to these systems, we look at a wide range of threats, including cyber, jamming, spoofing, supply chain challenges, space weather, and more.

The Space ISAC, like other ISACs, is led by and funded principally by its industry and academic members. The ISAC partners, however, with the public sector. We have in place MOUs with several US Government agencies, as well as space and cybersecurity government authorities in Australia, Canada, France, Greece, Germany, Israel, Taiwan, and the United Kingdom, and more partnerships are in progress, including a recent MOU with NATO.

We set up in 2023 an operational watch center in Colorado Springs, one that monitors threats to space systems using a wide range of data from our members, partners, and open sources. We use the DHS Traffic Light Protocol to control the dissemination of our reporting.

We've also announced global hubs in Australia, Canada, Japan, and the UK. As these global hubs become operational and as we build watch center components in these countries, the Space ISAC will gain 24/7, follow-the-sun coverage of the space systems environment, threats to that environment, and incidents that affect the security and resilience of that environment. Information about these and other Space ISAC developments can be found at the following link – place into my written testimony. https://spaceisac.org/newsroom/ We also convene working groups and task forces to examine and propose approaches to key space system security challenges, including space systems governance, analysis, quantum security, the security of cislunar operations, and other domains.

The Space ISAC has grown rapidly with over 120 members and we are also a member of the National Council of ISACs in the United States, as well as the EU Council of ISACs.

From the foregoing, I hoped to make clear a few key points.

First, the speed and scope with which we have operated and will continue to operate reflect our view that all critical infrastructures depend on space. While in 2019, there were approximately 2,00 active satellites, today we count over 14,500, with estimates ranging from 30,00 to as many as 60,000 satellites by 2030.

Surface and air transportation systems used space-based navigation. Maritime fleets also use space systems for navigation, as well as communication. Space systems provide timing data for our power grid.

Space-based remote sensing is vital to farming, including what we call “precision agriculture,” in which space-based systems help pinpoint areas for cultivation and fertilization. Financial systems depend on space infrastructure, with satellite technology providing high-precision timing for transaction timestamps, GPS for global synchronization, and secure data connectivity, particularly for remote ATMs and high-frequency trading. Space-based communications link remote locations, and commercial space systems are being used increasingly by our government for national security and civil government services. Industry now leads government in the number of space-based imagery platforms; global 5G networks, using thousands of satellites, are providing a worldwide, 5G IT “backplane.” So, the Space ISAC’s members and partners regard space systems as critical.

Second, much of the space systems domain is comprised of unique infrastructure, including manufacturing, launch, ground segment, and user segment systems. These infrastructures are growing rapidly; the Space ISAC and its members and partners believe we can brook no delay in the protection, security, and resilience of these supply chains. In addition, cislunar operations will be supported by their own unique infrastructures, including their own navigation satellites, and planning for the security of these new infrastructures should start now. In fact, the Space ISAC's cislunar affinity group is already working to define the security challenges associated with cislunar systems.

Third, our space systems represent a large and growing component of our national economy and that of allies and partners. Estimates vary, but we can expect to see at least $1T in space systems industry activity by, and possibly before 2030. And this number, does not by any means

consider the value of activity in other sectors, such as transportation, that use space system.

Next, new space system missions are evolving. We are likely to see cislunar and asteroid mining, new, commercial space stations (particularly as the ISS approaches decommissioning), energy production, and orbital cloud and data center services. Securing each of these missions, or lines of business, will pose its own challenges. As we build a new, global IT eco-system, one that encompasses space-based 5G networks, agentic AI-enabled systems that both collect and analyze imagery on orbit – and provide terrestrial users with suggested course of action, such as how best to get emergency relief to disaster victims – we will need to understand the threats posed to these systems, and how these systems can be secured and made resilient.

Cislunar operations, including mining, exploration, and even settlement, are becoming the focus of intense international rivalry, and will also need security.

Finally, the protection of our space systems – all of our space systems – is a global endeavor, one that requires to concerted effort of the United States, its allies, and partners.

To that end, the Space ISAC has been from its inception a global effort to include allies and partners with which we share values and, in some cases, space systems.

For example, our efforts with Australia and the UK reflect the overall collective security logic of AUKUS Pillar 2, with which we are aligned. Our efforts with other, likeminded countries, reflect the global nature of the space systems environment, and our mutual interdependence of the US and its allies and partners on each other's space systems.

Let's not forget that the attack by Russia on Ukraine was presaged a day before boots crossed the Ukrainian border by an attack on a commercial space system on which Ukraine depends, an attack that also disrupted electrical power in Germany and could have affected US users, too.

The Space ISAC itself tracked and reported to its members and partners on a satellite system in geospatial orbit that maneuvered against the blocked the transponders of commercial communication satellites, one of many incidents on which we share information. As the US works with its allies and partners in the collective defense of our space systems, we can also encourage the development of better behavioral norms. Adopted broadly, even our adversaries might well be compelled to recognize, and even possibly adopt these norms.

I am aware that debate is underway in the government regarding national space governance and how best to work with industry in support of the security of our space systems.

I am not here to recommend a government space systems security architecture, though I do believe a national R&D strategy and effort that unites industry, government, academia, and other stakeholders to identify, resource, and tackle space systems security and resilience challenges is warranted, if not overdue. Such a strategy, possibly coordinated with allies, and partners, could advance our ability to protect these systems, even as is brings together worthy efforts being undertaken in industry, academia, the IEEE, the National Institutes of Standards and Technology, and other stakeholders.

Let me add, in addition, that the Council on Foreign Relations Securing Space Task Force, of which I am a member, issued in 2025 a report[1] that noted: *"U.S. space assets are increasingly vulnerable to attacks by China, Russia, and other potential adversaries—attacks that could come from the ground, the air, or space itself."* The report recommended that *"the President should instruct relevant cabinet officers that the United States is to lead the world in space."* The report added: "*the President should structure the National Security Council staff to support the President in this role and the national effort to lead in space."*

In the meantime, the Space ISAC is moving ahead swiftly, coordinating, analyzing, and sharing as quickly as possible information needed to secure our space systems, critical

[1] See: https://www.cfr.org/task-force-reports/securing-space/introduction

to our national and economic security. Our efforts recognize the vital importance of our space systems. We're not waiting. Nor should our country.

Thank you again for this opportunity to share our progress and views. I look forward to your questions.

TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

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

RADM (RET.) MARK MONTGOMERY

Senior Director and Senior Fellow,
FDD's Center on Cyber and
Technology Innovation
Foundation for Defense of Democracies

Washington, DC
April 29, 2026

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chairman Ogles, ranking member, and distinguished members of the subcommittee, on behalf of the Foundation for Defense of Democracies, thank you for the opportunity to testify before you today.

The subject of this hearing is timely. Our nation is under attack in cyberspace. Our adversaries increasingly see this as a U.S. vulnerability, and China specifically is conducting "operational preparation of the battlefield" activities as well as espionage and intellectual property theft against our companies and critical infrastructure. At the same time, we appear to be reducing our investments in cyber defense.

National cyber resilience rests on three legs: a capable federal government able to mitigate, thwart, deter, and punish attackers; an informed private sector capable of defending itself from debilitating attacks; and robust public-private collaboration that facilitates rapid information transfer, a shared understanding of the threat landscape, and collective defense of the U.S. economy and national security.

Over the past year, the Trump administration has reduced funding for key offices and decommissioned collaboration mechanisms critical to both the first and the third pillars. But Congress has not done much better. While this subcommittee and the broader Homeland Security Committee have shown important leadership on cybersecurity issues, advancing numerous critical cybersecurity provisions, unrelated partisan fights and inter-chamber disagreements have blocked the passage and implementation of important legislation and left the Cybersecurity and Infrastructure Security Agency (CISA) — our national civilian cyber defense agency — operating at less than half its capacity.

As we have fumbled the ball, our adversaries have advanced down the field. China continues to pre-position destructive capabilities within our critical infrastructure. Just last week, the United States, its Five Eyes partners, and other U.S. allies warned that China's cyber operators are using covert, compromised networks "strategically, and at scale" to conduct their malicious campaigns.[1] Russia is maturing its kinetic and cyber anti-satellite capabilities to blind its adversaries. North Korea has infiltrated Fortune 500 companies by compromising the IT services industry. And Iran is launching not only cyberattacks but also drone and missile strikes against data centers in the region.

Countering these threats requires reinforcing the legs of the national cyber resilience table. A critical component of that reinforcement is before this committee today: how the federal government fulfills its commitments to the private sector. Most specifically, how does the Department of Homeland Security (DHS) support the resilience of the rapidly expanding and evolving components of the communications and information technology sectors: data centers, telecommunications networks, and space-based systems?

In addition to outlining the challenges our nation faces in cyberspace and the unique threats to these industries, my testimony lays out six recommendations for this subcommittee and your colleagues in Congress to improve CISA's ability to work with owners and operators to secure

the physical and virtual infrastructure that underpins America's national security and economic prosperity.

The Challenges

America's adversaries understand that holding U.S. critical infrastructure at-risk undermines our national security, economic prosperity, and public health and safety. They are taking advantage of our persistent under-investment in defense and resilience.

Adversarial Threats

Adversary infiltration of digital networks and the industrial processes they control is the most acute threat to the safety and security of the American citizenry and to the American way of life. Of the adversaries committed to endangering that which the United States holds dear, none looms larger than the Chinese Communist Party (CCP). Recent years have stripped away any remaining illusions about Beijing's ambition to displace the United States as the world's dominant power and about the depth and breadth of China's infiltration into American critical infrastructure — particularly through malicious cyber campaigns such as Volt Typhoon and Salt Typhoon.

The Chinese state-sponsored Volt Typhoon campaign is a calculated act of digital pre-positioning: CCP-linked hackers burrowed stealthily into U.S. systems — transportation networks, energy grids, and water utilities — not to strike immediately but to lie dormant until Beijing decides the moment is right.[2] As a military man, I call this "operational preparation of the battlefield." Senior U.S. intelligence officials have made clear that these implanted capabilities are designed to be activated during a future crisis, with the goals of disrupting military logistics, inciting societal panic, and slowing Washington's ability to respond.

Meanwhile, Salt Typhoon is a direct assault on American and allied communications networks. Operated by the CCP's Ministry of State Security, the group has conducted a pervasive cyber espionage campaign in the United States and other Western allied nations.[3] The campaign successfully infiltrated at least nine U.S. telecommunications networks and internet service providers, including AT&T, Verizon, and T-Mobile,[4] among other things, compromising networks that support law enforcement and the intelligence community in their work conducting court-approved wiretaps under the Communications Assistance for Law Enforcement Act.[5] Among the stolen data were audio recordings of phone calls between high-ranking U.S. government officials.[6] The exact number of compromised telecommunications companies remains unconfirmed, but the FBI warned earlier this year that the threat posed by Salt Typhoon is "still very, very much ongoing."[7]

America's other adversaries are also on the march — Russia, Iran, and North Korea continue their persistent and pervasive cyber campaigns against the United States and our allies and partners. Russia is pummeling democratic, pro-American Ukraine with missile and cyberattacks while harboring criminal gangs that extort American hospitals, as the committee heard last week.[8] North Korea — which functions less like a conventional nation-state and more like a criminal enterprise with a flag — has established a niche in large-scale cryptocurrency theft. Its

operatives have penetrated Fortune 500 companies by stealing identities, leveraging artificial intelligence, and posing as IT workers.[9] Iran is targeting industrial control systems, and Tehran's attacks are causing "operational disruption and financial loss," the FBI and other federal agencies warned earlier this month.[10] Over the course of the war, the Islamic Republic also used its drone and missile arsenal to damage American data centers in the region — a particularly troubling development given the importance of this infrastructure for America's artificial intelligence investment and trade priorities.

America's communications networks are also vulnerable to criminal sabotage. In September, the U.S. Secret Service dismantled a SIM farm in the New York City area that officials said could have overwhelmed and shut down the city's telecommunications networks, including emergency services.[11] While the investigation is ongoing and the network was likely criminal, law enforcement warned it may have a nation-state nexus.[12]

Self-Imposed Weaknesses

Thwarting America's adversaries in cyberspace would be hard enough given America's exposure through highly networked, but insecure, systems and our adversaries' investments in malicious cyber activities. Indeed, I have testified before this committee in the past that no presidential administration has properly invested in the cybersecurity of our national critical infrastructures. But it is my assessment that over the past year, the federal government has undercut its own capabilities even further. This is despite the fact that this president's National Security Strategy made it clear that threats to the homeland — including cyber threats — were a priority that needed to be addressed.

Last year, then-Secretary of Homeland Security Kristi Noem suspended the Critical Infrastructure Partnership Advisory Council (CIPAC) as part of Trump's general restructuring of Biden-era advisory councils across the federal government. Readjustments of membership on advisory councils are expected at the transition to a new administration, but CIPAC was different. It was a convening authority that gave federal agencies, critical infrastructure companies, and trade groups a way to hold strategic conversations on sensitive information about cyber and physical vulnerabilities. It provided an essential bridge between government and private companies by offering legal protection and a convening body for Sector Coordinating Councils to meet with the government.[13]

After CIPAC's suspension, leaders across critical infrastructure sectors canceled meetings and refused to share findings from a cyber working group — limiting the private-public cooperation necessary to ensure critical infrastructure is prepared to face adversarial cyberattacks.[14] Testifying before the House Committee on Energy and Commerce, industry representatives urged DHS to move forward with CIPAC's intended replacement, the Alliance of National Councils for Homeland Operational Resilience (ANCHOR).[15] But since January, there have been no updates. We have now gone more than a year without a tool that is critical for government support for public-private collaboration.

This administration has undermined the capabilities of its own civilian cyber defense agency. President Trump created CISA, but his administration, through the actions of both DOGE and

DHS itself, seems bent on weakening it. Its workforce decisions have resulted in a vacancy rate of 40 percent in key mission areas, according to CISA's own assessment.[16] And just this month, we learned that the president's fiscal year 2027 budget proposal calls for an additional $707 million reduction in funding for CISA's work.[17]

This proposed cut has a direct bearing on CISA's ability to serve as a sector risk management agency (SRMA). Five years ago, Congress expanded the responsibilities of federal agencies to help critical infrastructure owners and operators identify and mitigate threats, evaluate risks, and respond to incidents.[18] These agencies, dubbed SRMAs, need expertise in both the cyber threat landscape and in the operation of the sector for which they are responsible.

DHS is the SRMA or co-SRMA for 10 of the 16 critical infrastructure sectors and has delegated the execution of these duties for nine sectors to CISA.[19] In this role, CISA is supposed to identify risks to the sector and coordinate with other relevant agencies, owners and operators, and state, local, tribal, and territorial entities to ensure sector security. It is nigh impossible to do this work when the department halves the budget of its own risk management activities and reduces its stakeholder engagement capabilities by $58 million — a 65 percent cut.[20] Last year, press reporting confirmed that the agency had essentially shuttered its Stakeholder Engagement Division, reducing its staff by as much as 95 percent.[21] While CISA officials claim that they are still able to fulfill their mission, in my 40 years in the Navy and in government, I never once had a subordinate say, "I could do my job better if you cut my budget and staff by half." We would NEVER consider such a reduction to the nation's military cyber defense agency.

Prior to this latest round of budget and staffing cuts, CISA and the other SRMAs long struggled to execute their duties. A 2023 Government Accountability Office report found that SRMAs had insufficient funding to execute their mission.[22] If you ask subject matter experts within DHS — to the extent that the department has retained its critical infrastructure experts — I suspect they would report that they are even more critically underfunded and understaffed.

Multiple GAO reports recommend that CISA and other SRMAs develop methods for determining how well sectors are implementing standards and procedures, noting that most agencies have not done so.[23] Since 2010, GAO has made 106 public recommendations related to federal and critical infrastructure cybersecurity.[24] Dozens remain outstanding.

Among the most critical infrastructure sectors under CISA's watch are the communications and information technology sectors. These two sectors are uniquely important. They are interconnected with and serve as the underlying infrastructure for other sectors. Each encompasses a wide range of services, and over the past decade since the executive branch last updated the definitions of critical infrastructure sectors, they have undergone some of the most dramatic technological changes of all the critical infrastructure sectors.

Arguably, technological innovation has muddled the distinction between the communications and information technology sectors. They are increasingly intertwined and encompass similar assets. Data centers and cloud infrastructure, for example, fall in part under both sectors. Recognizing the connectivity between the sectors back in 2018, DHS created a task force on information and communications technology supply chain management. It was co-chaired by

CISA and the Information Technology and Communications Sector Coordinating Councils. The task force was charged with "devising realistic, actionable, and risk-based" solutions to the challenges facing the two sectors, but it expired in January of this year and is in a holding pattern awaiting DHS action.[25]

I applaud the subcommittee for looking at the three unique and critical components of both these sectors: data centers, telecommunications networks, and space-based systems. If our nation does not properly secure these assets, our adversaries will steal, corrupt, and disrupt the data and communications that allow our economy to function.

Data Centers

Data centers and cloud infrastructure are becoming more vital to American economic prosperity and our society writ large due to their important role in enabling internet systems, telecommunications systems, and many online services. The explosion of AI innovation has catapulted debates about the construction of data centers into the national spotlight. The cyber and physical resilience of these facilities merits the same level of attention.

Data centers are sites that house and manage the IT infrastructure and data used to build, run, and deliver applications and services.[26] The number of data centers is increasing, and many are owned by major cloud service providers that provide remote access to their services. Hyperscale data centers (known as hyperscalers) are data centers that are big enough to handle large workloads through an optimized network infrastructure. Hyperscalers are especially useful for artificial intelligence, automation, and the handling of big data.[27]

The proliferation of data centers is increasing the demand for electricity and leading to the digitization of the grid. A modern grid has the ability to be more responsive to demand fluctuations and more resilient against cyberattacks, but not if we embed Chinese-made components at critical control layers. Understanding risks and prioritizing mitigations requires collaboration between hyperscalers, energy providers, and the federal government, as well as between the Department of Energy and CISA.

The data center industry itself is concentrated. The top three providers — Amazon Web Services, Microsoft Azure, and Google Cloud Platform — together account for 63 percent of the market share.[28] The reliance of critical services on concentrated infrastructure introduces security concerns. For example, close to 70 percent of all global internet traffic runs through data centers in Northern Virginia.[29] An October 2025 internal disruption to domain name service protocols impacting one Amazon Web Services region caused outages across consumer apps, core Amazon operations, financial platforms, and enterprise services — including Amazon.com, Venmo, Coinbase, Snapchat, and more.[30] The outage also impacted multiple communications and transportation providers, including AT&T, Delta Airlines, Lyft, Signal, Spectrum, and Zoom.[31] Even global banks were affected.[32] An outage lasting less than a day may have cost the global economy billions of dollars.[33]

And this outage was a simple misconfiguration. Had the service been sabotaged by malicious actors, the disruption would have been longer and worse.

Iran is already testing its hand at this. In March 2026, Iran targeted two Amazon Web Services data centers in the Middle East, claiming the attack sought to "identify the role of these centers in supporting the enemy's military and intelligence activities."[34] While the attack on one center did not substantially disrupt services, the second strike led to civilian impacts for millions of people in Dubai and Abu Dhabi who were unable to access transportation, food delivery, and financial services due to the outage.

Let me repeat: Iran used drones to attack an American company to attempt to degrade our military capabilities. While the strikes failed in their stated mission, Moscow and Beijing are no doubt watching. Both are more likely to launch cyberattacks than missile strikes on the U.S. homeland, but both are also increasing the size and sophistication of their missile systems.

Telecommunications

Over the past year, the Federal Communications Commission (FCC) has reinvigorated its national security mission. This has been the single most important administration effort to deal with emerging technology challenges from China. The FCC has long managed an effort to remove Huawei and ZTE equipment from U.S. networks and has banned state-owned Chinese telecommunications companies from providing services in the United States.[35] Over the past year, the FCC has further leveraged its regulatory authority to prohibit the sale of Chinese-made connected devices in the United States over national security concerns. This is vital national security work, but it does not diminish what CISA must do as the SRMA for the communications sector.

Banning Chinese telecommunications equipment is important, but in the case of Salt Typhoon, the access vector was Cisco routers. This American-made equipment contained vulnerabilities that Chinese hackers exploited. Critical infrastructure is not just about who manufactures the hardware but also about whether the manufacturers and the operators properly maintain it.

Indeed, Salt Typhoon remains the most pressing threat to the American telecommunications industry. In early 2025, CISA warned that there had been no confirmation that Salt Typhoon had been fully evicted from compromised networks.[36] The FBI has since also stated publicly that the threat is ongoing.

Mitigating the Salt Typhoon threat has been hampered by government failures. Four years ago, CISA conducted a study on cyber vulnerabilities in telecommunications systems. Despite pledging to Congress that it would release the findings, CISA has yet to do so.[37] A joint public-private study on Salt Typhoon has similarly been buried. At the same time that the Trump administration dissolved CIPAC, it also disbanded the Cyber Safety Review Board.[38] The board — comprising representatives from government and from private industry — had been in the middle of investigating the Salt Typhoon hacks. Dissolving the board leaves dire lessons unlearned and the American public still unaware of the degree to which their communications were compromised. The subcommittee has a critical obligation to determine the status of this work and when the American people can expect to see the findings.

I am concerned that these failures are symptomatic of a greater problem in CISA's ability to carry out its SRMA duties for the communications sector. A 2021 GAO study concluded CISA's SRMA work for the communications sector needed significant improvement.[39] In particular, GAO warned that while CISA had programs to support the communications sector, it had not assessed the effectiveness or comprehensiveness of this effort. That recommendation remains open, meaning to this day, CISA does not know if the agency is actually useful to the sector.

GAO also urged CISA to update the "sector-specific plan" for the communications sector — the plan that lays out how the government will perform its SRMA duties to help critical infrastructure owners and operators identify and mitigate threats, evaluate risks, and respond to incidents. To this day, the most recent publicly available sector-specific plan dates to 2015.[40] Suffice it to say, many things have changed in the past 10 years. Back in 2021, CISA conceded to GAO that updating the plan was already two years behind schedule and that "certain elements of the plan [were] out of date."[41] In September 2025, CISA finally provided GAO with a copy of the new plan. It appears, however, that the new Risk Management Plan is not available publicly online. What good is an updated plan if owners and operators cannot easily find it?

Space-based Systems

Within the communications sector, it is the security of satellite communications and other space-based assets that gives me the greatest heartburn. After all, one of the first volleys in the Ukraine war was a Russian cyberattack against an American satellite communications company.[42]

CISA's interactions with satellite communications companies give it just a fraction of the picture of what is happening hundreds of miles above us. Since the end of the Cold War, the United States has largely been unchallenged in outer space, but that is changing quickly. Moscow and Beijing are becoming more invested in space because they know that those who can exert influence beyond Earth hold unparalleled power on it. Space systems underpin critical commercial and government functions, not just satellite communications but also missile defense. The Global Positioning System is integral to everything from crop irrigation to grid synchronization to global financial transactions.

China and Russia have both asserted that commercial space systems can be legitimate military targets,[43] and they are acting on this doctrine. America's adversaries possess counterspace weapons with capabilities ranging from temporarily disabling satellites to manipulating trajectories or onboard processes to complete kinetic destruction of the satellite.[44] Our adversaries are prepared to use cyberattacks, electronic jamming and spoofing, anti-satellite missiles, and co-orbital systems to degrade our capabilities. Just last year, then-Vice Chief of Space Operations General Michael Guetlein warned that our near-peer adversaries are "practicing dogfighting in space with satellite-on-satellite" operations.[45]

This extraterrestrial competition will only intensify. Three years ago, China announced plans to send a crewed mission to the moon before 2030 to rival NASA's Artemis program.[46] The next year, Moscow and Beijing announced a joint program to construct a lunar base by 2035, again competing with U.S. timelines. The two countries signed an agreement to build a lunar nuclear power plant, challenging NASA's plans to launch a reactor by the early 2030s. NASA warned

last year that if our adversaries beat us to the punch, they will, in essence, "declare a keep-out zone which would significantly inhibit the United States."[47]

The consequences of failing to protect U.S. space systems — and ceding space superiority to adversaries — would be detrimental to national security.[48] CISA's narrow insights into satellite communications do not provide it with the perspective to understand the full scope of risks to space-based assets. This is why I, along with my colleague Frank Cilluffo, continue to endorse designating space systems as a U.S. critical infrastructure sector so that these assets that are vital to U.S. national security, economic prosperity, and public health and safety receive the policy attention and risk management support they deserve.[49] Today, governance and support is fragmented across CISA, NASA, Commerce, the Pentagon, and other federal agencies and state authorities.[50]

Despite the fact that in a 2021 report — a report demanded by Congress — CISA acknowledged that space systems should be designated as a critical infrastructure sector,[51] the Biden administration failed to act. This Congress and the Trump administration have an opportunity to secure American space-based systems by designating them as critical infrastructure. Failing to do so will have serious national security consequences as our adversaries pursue deliberate efforts to erode U.S. space superiority.

Recommendations

Ensuring the resilience of America's communications and IT infrastructure is essential for our nation's continued prosperity. While private companies must invest in their own cybersecurity, they cannot reinforce America's cyber resilience alone. Critical infrastructure owners and operators need competent government partners. Core to that partnership is the SRMA structure. Congress can ensure that CISA is resourced and structured correctly for this mission.

1. **Fully fund CISA for its SRMA and national coordinator mission and require CISA to conduct a force structure assessment.**

Last year, the president's budget proposed cutting 17 percent of CISA's funding, putting the agency's budget at about $2.3 billion.[52] Congress disagreed with such a dramatic cut, and appropriators were on track earlier this year to provide CISA with $2.6 billion.[53] This year, the president's budget again proposes to cut CISA's funding, this time by over $700 million[54] — leaving what the former chairman of this committee, Rep. John Katko, used to say should be a $5 billion agency[55] with just over $2 billion to execute its mission. Congress should once again reject the president's dramatic cuts to CISA and fund the agency to meet its mission as both the SRMA for nine sectors as well as the national coordinator for critical infrastructure resilience.

Reasonable people can disagree about the precise funding level CISA needs, but Congress needs an objective answer. As such, lawmakers should request a force structure assessment of the agency to determine its ability to fulfill statutory requirements. In Section 1745 of the FY 2021 National Defense Authorization Act,[56] Congress demanded CISA conduct just such an assessment. For three years, the Biden administration tried and failed to do this assessment, leaving the incoming Trump administration with no roadmap for agency development, and from

there, things only got worse. Lawmakers should demand this assessment again. Armed with that information, Congress and the White House can determine how CISA should be organized and what level of funding is appropriate.

2. Request an update from DHS on its efforts to replace CIPAC.

Since January, the department has provided no concrete updates on its plans to replace CIPAC. At that time, some press reporting indicated that the ANCHOR plan was on the secretary's desk for final approval. I suspect that was an overly optimistic description of its status, but nonetheless, less than eight weeks later, Secretary Kristi Noem was out. Newly confirmed Secretary Markwayne Mullin should update Congress on his plans to undo the damage his predecessor did by dissolving CIPAC. This subcommittee should request a briefing from the department and ensure the mechanism DHS implements provides for maximum collaboration and trusted information sharing among private and public entities.

3. Demand that the White House nominate a CISA director.

For the past 15 months, CISA has operated without a Senate-confirmed director. Sean Plankey was extremely qualified and would have made a fine director. After it became abundantly clear that the Senate would not confirm him — because of unrelated issues to do with the Coast Guard — he withdrew his nomination last week. The White House should promptly announce a new nominee and work with the Senate to confirm that individual as soon as possible. Members of this committee should remind their Senate counterparts and the White House that without a confirmed director, the nation's civil defense agency cannot execute the administration's strategy to "act swiftly, deliberately, and proactively to disable cyber threats to America."[57]

4. Designate space systems as critical infrastructure and NASA as its SRMA.

Congress should designate space systems as critical infrastructure. This is not about regulating the industry but rather about making sure that the federal government is organized and on mission to support the identification and mitigation of risks to the sector. It would establish a formal structure with clearly defined roles and authorities, improve understanding of threats, and enhance private-public collaboration.

Critics argue that such a designation is too complex due to cross-sector entanglement, but that is precisely why it is necessary. Space systems encompass the ecosystem from the ground to orbit, including sensors, signals, data, payloads, and supply chains. "Space-based assets are part of the nation's critical infrastructure and are increasingly integrated into daily life," CISA's executive assistant director for infrastructure security, Steve Casapulla, noted earlier this month.[58] Congress should make this official, establishing space as the 17th critical infrastructure sector and signaling to adversaries that Washington considers these systems essential and that it will defend them accordingly.

Alongside this designation, Congress should assign the SRMA duties to NASA. Managing risk in this sector requires expertise in national security, economic analysis, science and technology, and space operations — areas in which NASA has deep experience. NASA should serve as the

central coordinating authority, supported by additional funding to scale its capacity. Two subgroups should operate under NASA: one focused on the military and the intelligence community and another on civilian satellite communications. The Pentagon would continue to lead within its domain, while CISA — as SRMA for communications — would continue to engage with the latter. Congress should not, however, assign NASA a regulatory role. Existing regulatory frameworks already govern space systems; adding another layer would likely increase inefficiency rather than security.

5. **Require CISA to explain its assessment of the distinction between the communications and IT sectors.**

Decade-old sector-specific plans mean that Congress — and the American people — do not know how CISA assesses the risks to and the makeup of the communication and IT sectors. Congress should require CISA to provide an assessment of the position of data centers and cloud infrastructure within the current critical infrastructure sector frameworks. These systems are possibly the fastest-growing component of the IT sector while becoming increasingly inseparable from the communications sector. Understanding CISA's current approach and collaborative work across the IT and communications sectors to secure data centers can inform Congress as to whether stronger support is needed to improve the resilience of these systems.

6. **Require SRMAs to update sector-specific plans or sector risk management plans biennially and DHS to update the national plan.**

Since 2021, CISA's efforts to update the communications sector-specific plan — and the risk management plans for the other sectors — have been repeatedly delayed by efforts to update the National Infrastructure Protection Plan (NIPP). Disgracefully, the last finalized version of the NIPP we have is from 2013. Over the decade and a half since then, DHS has attempted in fits and starts to update the national plan, pledging in 2024 to release the first biennial National Infrastructure Risk Management Plan the following year.[59] Needless to say, it hasn't. The Trump administration announced a much-needed review of all critical infrastructure policies, including National Security Memorandum 22, which set forward biennial deadlines for new sector and national plans.[60] If the executive branch cannot keep to its self-imposed deadlines, Congress needs to step in. Lawmakers should amend the legislation creating the tasking for SRMAs to include a requirement to update sector plans biennially and for CISA to issue a national plan — as well as the National Cyber Incident Response Plan — every two years.

Conclusion

Americans need food, water, and electricity to live. Our economy needs data and the internet. The military needs a networked transportation system to have the mobility to get to the fight. The IT and communications sectors are not just critical infrastructure but also essential infrastructure to each of these missions — public health and safety, economic prosperity, and national security. Their resilience against cyber and physical threats requires robust collaboration between the government and private companies. Washington has been failing to live up to its side of the arrangement for decades. Congress must take action to change that.

Thank you for the invitation to testify. I look forward to your questions.

[1] Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, "Defending against China-nexus covert networks of compromised devices," April 23, 2026. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a)
[2] "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," *Federal Bureau of Investigation*, April 18, 2024. (https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says); Christopher Wray, "The CCP Cyber Threat to the American Homeland and National Security," *U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party*, January 31, 2024. (https://www.fbi.gov/news/speeches-and-testimony/the-ccp-cyber-threats-to-the-american-homeland-and-national-security)
[3] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise," January 17, 2025. (https://home.treasury.gov/news/press-releases/jy2792); Greg Otto, "Malware linked to Salt Typhoon used to hack telcos around the world," *CyberScoop*, November 25, 2024. (https://cyberscoop.com/salt-typhoon-us-telecom-hack-earth-estries-trend-micro-report)
[4] Sarah Krouse and Dustin Volz, "T-Mobile Hacked in Massive Chinese Breach of Telecom Networks," *The Wall Street Journal,* November 15, 2024. (https://www.wsj.com/politics/national-security/t-mobile-hacked-in-massive-chinese-breach-of-telecom-networks-4b2d7f92)
[5] Martin Matishak, "US adds 9th telecom company to list of known Salt Typhoon targets," *The Record*, December 27, 2024. (https://therecord.media/nine-us-companies-hacked-salt-typhoon-china-espionage)
[6] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise," January 17, 2025. (https://home.treasury.gov/news/press-releases/jy2792); Greg Otto, "Malware linked to Salt Typhoon used to hack telcos around the world," *CyberScoop*, November 25, 2024. (https://cyberscoop.com/salt-typhoon-us-telecom-hack-earth-estries-trend-micro-report)
[7] Derek B. Johnson, "FBI: Threats from Salt Typhoon are 'still very much ongoing,'" *CyberScoop*, February 19, 2026. (https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026)
[8] Cynthia Kaiser, "Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans," *Testimony before the House Subcommittee on Border Security and Enforcement and the House Subcommittee on Cybersecurity and Infrastructure Protection*, April 21, 2026. (https://homeland.house.gov/hearing/online-scams-crypto-fraud-and-digital-extortion-an-examination-of-how-transnational-criminal-networks-target-americans)
[9] Matt Kapko, "North Korean Operatives have infiltrated hundreds of Fortune 500 companies," *CyberScoop*, April 30, 2025. (https://cyberscoop.com/north-korea-workers-infiltrate-fortune-500)
[10] U.S. Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure," April 7, 2026. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a)
[11] Joseph De Avila and James Fanelli, "Secret Service Thwarts Telecom Threat in NYC Area Ahead of U.N. General Assembly," *The Wall Street Journal,* September 23, 2025. (https://www.wsj.com/politics/national-security/un-secret-service-electronic-device-network-8d30e7de)
[12] Shawn Chen and Julie Walker, "How 'SIM farms' like the one found near the UN could collapse telecom networks," *Associated Press,* September 23, 2025. (https://www.pbs.org/newshour/nation/how-sim-farms-like-the-one-found-near-the-un-could-collapse-telecom-networks)
[13] Mark Montgomery and Johanna Yang, "Stop Gutting America's Cyber Defense Agency," *The Hill,* March 26, 2025. (https://thehill.com/opinion/cybersecurity/5214315-stop-gutting-americas-cyber-defense-agency)
[14] Eric Geller, "'Suspended animation': US government upheaval has frayed partnerships with critical infrastructure," *Cybersecurity Dive*, June 25, 2025. (https://www.cybersecuritydive.com/news/critical-infrastructure-cybersecurity-partnerships-disruption-trump-government-industry/751589)
[15] Mark Montgomery and Aarushi Garg, "Cyber Information Sharing Must Be Fixed or our Adversaries Reap the Benefits," *Threat Beat,* February 1, 2026. (https://www.fdd.org/analysis/2026/02/01/cyber-information-sharing-must-be-fixed-or-our-adversaries-reap-the-benefits-2)
[16] Lily Hay Newman, "Fears Mount That US Federal Cybersecurity Is Stagnating -- or Worse," *WIRED,* December 31, 2025. (https://www.wired.com/story/expired-tired-wired-federal-cybersecurity)

[17] U.S. Department of Homeland Security, "Cybersecurity and Infrastructure Security Agency Budget Overview Fiscal Year 2027 Congressional Justification," April 2025. (https://www.dhs.gov/sites/default/files/2026-04/26_0403_ocfo-budget-cisa.pdf)
[18] Mary Brooks, Annie Fixler, and Mark Montgomery, "Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure," *CSC 2.0*, June 7, 2023. (https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure)
[19] "Sector Risk Management Agencies," *Cybersecurity and Infrastructure Security Agency*, accessed April 24, 2026. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies)
[20] Nick Anderson, "The Fiscal Year 2027 Budget for the Cybersecurity and Infrastructure Security Agency," *Testimony before the House Appropriations Committee Subcommittee on Homeland Security,* April 16, 2026. (https://docs.house.gov/meetings/AP/AP15/20260416/119152/HHRG-119-AP15-Wstate-AndersenN-20260416.pdf)
[21] Eric Geller, "CISA's international, industry and academic partnerships slashed," *Cybersecurity Dive,* October 22, 2025. (https://www.cybersecuritydive.com/news/cisa-stakeholder-engagement-division-layoffs-critical-infrastructure-international/803433)
[22] U.S. Government Accountability Office, "Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities," February 2023, page 23. (https://www.gao.gov/assets/gao-23-105806.pdf)
[23] U.S. Government Accountability Office, "Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance," February 9, 2022. (https://www.gao.gov/products/gao-22-105103)
[24] U.S. Government Accountability Office, "Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure," February 7, 2023. (https://www.gao.gov/products/gao-23-106441)
[25] "Information and Communications Technology Supply Chain Security," *Cybersecurity and Infrastructure Security Agency*, accessed April 24, 2026. (https://www.cisa.gov/topics/information-communications-technology-supply-chain-security); Cybersecurity and Infrastructure Security Agency, Press Release, "CISA Announces Renewal of the Information and Communications Technology Supply Chain Risk Management Task Force," February 6, 2024. (https://www.cisa.gov/news-events/news/cisa-announces-renewal-information-and-communications-technology-supply-chain-risk-management-task)
[26] Stephanie Susnjara and Ian Smalley, "What is a data center?" *IBM*, accessed February 24, 2026. (https://www.ibm.com/think/topics/data-centers)
[27] Phill Powell and Ian Smalley, "What is a hyperscale data center?" *IBM*, accessed April 24, 2026. (https://www.ibm.com/think/topics/hyperscale-data-center)
[28] Cody Slingerland, "21+ Top cloud Service Providers Globally in 2026," *CloudZero*, March 3, 2026. (https://www.cloudzero.com/blog/cloud-service-providers)
[29] Katherine Hafner, "Data centers keep growing in Virginia -- and so does energy demand," *WHRO*, November 14, 2024. (https://www.vpm.org/news/2024-11-14/meta-google-amazon-dominion-energy-data-centers-virginia-power-demand)
[30] Matt Pusatory and Matt Gregory, "AWS outage puts Northern Virginia data centers in the spotlight," *WUSA9,* October 20, 2025. (https://www.wusa9.com/article/tech/amazon-web-services-outage-puts-northern-virginia-data-centers-spotlight/65-9e547d6c-1669-40dd-8cd1-c175f45ce563#:~:text=Ripple%20effect,and%20Venmo%20temporarily%20halted%20transactions)
[31] Michael Grothaus, "AWS outage hits much of the internet, impacting a long list of websites and apps, from Reddit to McDonald's," *Fast Company,* October 20, 2025. (https://www.fastcompany.com/91425038/aws-outage-today-list-of-websites-hit-us-east-1-amazon-down)
[32] Liv McMahon, "Amazon apologises to customers impacted by huge AWS outage," *BBC* (UK)*,* October 23, 2025. (https://www.bbc.com/news/articles/cvgvnp77dy9o)
[33] Jon Tran, "The Cloud is Falling: AWS Outage and Why it Matters," *The Chertoff Group,* October 22, 2025. (https://chertoffgroup.com/aws-outage-why-it-matters)
[34] Daniel Boffey, "'It means missile defence on datacentres': drone strikes raise doubts over Gulf as AI superpower," *The Guardian* (UK)*,* March 7, 2026. (https://www.theguardian.com/world/2026/mar/07/it-means-missile-defence-on-data-centres-drone-strikes-raises-doubts-over-gulf-as-ai-superpower)
[35] Federal Communications Commission Wireline Competition Bureau, "Secure and Trusted Communications Networks Reimbursement Program Sixth Report," June 30, 2025. (https://docs.fcc.gov/public/attachments/DOC-412591A1.pdf); U.S. House of Representatives Select Committee on the Chinese Communist Party, Press Release, "House Committee Subpoenas Chinese Telecom Giants After Refusal to Disclose CCP and Military Links," April

24, 2025. (https://chinaselectcommittee.house.gov/media/press-releases/house-committee-subpoenas-chinese-telecom-giants-after-refusal-disclose-ccp)
[36] Mark T. Hoske, "How to mitigate the ongoing Salt Typhoon telecom hack: CISA," *Control Engineering,* February 12, 2025. (https://www.controleng.com/how-to-mitigate-the-ongoing-salt-typhoon-telecom-hack-cisa)
[37] Tim Starks, "CISA says it will release telecom security report sought by Sen. Wyden to lift hold on Plankey nomination," *CyberScoop,* July 29, 2025. (https://cyberscoop.com/cisa-says-it-will-release-telecom-security-report-sought-by-sen-wyden-to-lift-hold-on-plankey-nomination)
[38] David Jones, "DHS disbands existing advisory board memberships, raising questions about CSRB," *Cybersecurity Dive,* January 22, 2025. (https://www.cybersecuritydive.com/news/dhs-disbands-advisory-board-csrb/737976/)
[39] U.S. Government Accountability Office, "Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector," November 23, 2021. (https://www.gao.gov/products/gao-22-104462)
[40] "Communications Sector," *Cybersecurity and Infrastructure Security Agency*, accessed February 24, 2026. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector)
[41] U.S. Government Accountability Office, "Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector," November 23, 2021. (https://www.gao.gov/products/gao-22-104462)
[42] UK Foreign, Commonwealth and Development Office, Press Release, "Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion," May 10, 2022. (https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion)
[43] Sandra Erwin, "Russia escalates rhetoric on commercial satellites, calls them 'legitimate targets for retaliation,' *Space News*, October 27, 2022. (https://spacenews.com/russia-escalates-rhetoric-on-commercial-satellites-calls-them-legitimate-targets-for-retaliation); U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025," 2025, page 21. (https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF#page=21)
[44] Emmanouil M. Karatarakis, "America's Intelligence Satellites are Proliferating: Their Protection is Not, With Exceptions," *The Cipher Brief,* January 30, 2026. (https://www.thecipherbrief.com/americas-intelligence-satellites-are-proliferating-their-protection-is-not-with-exceptions)
[45] Audrey Decker, "China is practicing 'dogfighting' in space, Space Force says," *Defense One,* March 18, 2025. (https://www.defenseone.com/threats/2025/03/china-practicing-dogfighting-space-space-force-says/403863)
[46] Emmerson Overell, "Houston, Americans Are Headed Back to the Moon," *Foundation for Defense of Democracies,* March 27, 2026. (https://www.fdd.org/analysis/2026/03/27/houston-americans-are-headed-back-to-the-moon)
[47] Sam Skove, "Duffy to announce nuclear reactor on the moon," *Politico,* August 4, 2025. (https://www.politico.com/news/2025/08/04/nasa-china-space-station-duffy-directives-00492172)
[48] Mark Montgomery, Craig Singleton, Jack Burnham, and Sophie McDowall, "Space Modernization for the 21st Century," *Foundation for Defense of Democracies,* October 28, 2025. (https://www.fdd.org/analysis/2025/10/28/space-modernization-for-the-21st-century)
[49] Frank Cilluffo, Mark Montgomery, Sharon Cardash, and Kelsey Shields, "Time to Designate Space Systems as Critical Infrastructure," *CSC 2.0,* April 14, 2023. (https://cybersolarium.org/csc-2-0-reports/time-to-designate-space-systems-as-critical-infrastructure); Georgianna Shea and Humza Khan, "Critical Orbit: The Case for Designating Space as National Critical Infrastructure in the Cyber Age," *CPI TechReg Chronicle,* July 30, 2025. (https://www.fdd.org/analysis/2025/07/30/critical-orbit-the-case-for-designating-space-as-national-infrastructure-in-the-cyber-age)
[50] Anne Wainscott-Sargent, "It's Unanimous: Space Already Functions as Critical Infrastructure," *Via Satellite,* April 7, 2026. (https://interactive.satellitetoday.com/via/april-may-2026/its-unanimous-space-already-functions-as-critical-infrastructure)
[51] U.S. Department of Homeland Security, "FY 2021 National Defense Authorization Act Section 9002(b) Report," November 12, 2021, page 44 (https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf)
[52] Eric Geller, "Trump proposes major cut to CISA's budget, citing false 'censorship' claims," *Cybersecurity Dive*, May 2, 2025. (https://www.cybersecuritydive.com/news/trump-cisa-budget-cuts-disinformation/747047); Weslan

Hansen, "House Panel Softens CISA Budget Cut to 4.6%," *MeriTalk*, June 11, 2025. (https://www.meritalk.com/articles/house-panel-softens-cisa-budget-cut-to-4-6)
[53] Tim Starks, "Congressional appropriators move to extend information-sharing law, fund CISA," *CyberScoop*, January 20, 2026. (https://cyberscoop.com/congressional-appropriators-move-to-extend-information-sharing-law-fund-cisa)
[54] Jiwon Ma, "America's Cyber Strategy Has a Budget Problem," *The Cipher Brief,* April 23, 2026. (https://www.thecipherbrief.com/americas-cyber-strategy-budget-problem)
[55] Jory Heckman, "Katko calls for $5B CISA budget to reflect its 'quarterback' status," *Federal News Network*, March 22, 2021. (https://federalnewsnetwork.com/cybersecurity/2021/03/katko-calls-for-5b-cisa-budget-to-reflect-its-quarterback-status)
[56] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4138. (https://www.congress.gov/bill/116th-congress/house-bill/6395/text/statute)
[57] "President Trump's Cyber Strategy for America," *The White House*, March 2026. (https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf)
[58] Anne Wainscott-Sargent, "It's Unanimous: Space Already Functions as Critical Infrastructure," *Via Satellite,* April 7, 2026. (https://interactive.satellitetoday.com/via/april-may-2026/its-unanimous-space-already-functions-as-critical-infrastructure)
[59] U.S. Department of Homeland Security, Memorandum, "Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025)," June 14, 2024. (https://www.dhs.gov/sites/default/files/2024-06/24_0620_sec_2024-strategic-guidance-national-priorities-u-s-critical-infrastructure-security-resilience.pdf); Jen Easterly, "A Plan to Protect Critical Infrastructure from 21st Century Threats: Purpose of the National Infrastructure Risk Management Plan," *Cybersecurity and Infrastructure Security Agency*, May 29, 2024. (https://www.cisa.gov/news-events/news/plan-protect-critical-infrastructure-21st-century-threats)
[60] Executive Order 14239, "Achieving Efficiency Through State and Local Preparedness," March 19, 2025. (https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness)

Prepared Testimony of Robert Mayer

Senior Vice President, Cybersecurity & Innovation, USTelecom — The Broadband Association

Before the House Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

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

April 29, 2026

Chairman Garbarino, Ranking Member Thompson, Chairman Ogles and Members of the Subcommittee, thank you for the opportunity to appear before you today.

I am Robert Mayer, Senior Vice President of Cybersecurity and Innovation at USTelecom and Chair of the Communications Sector Coordinating Council. I also serve as the Co-chair of the Department of Homeland Security ICT Supply Chain Risk Management Task Force.

USTelecom represents companies that build, operate, and secure the communications networks that underpin the American economy and support every sector of critical infrastructure. As communications networks and information technology systems become increasingly interconnected, ensuring their security depends on strong coordination, clear roles, and trusted public-private partnerships.

I will focus my remarks on three areas: our partnership with the Cybersecurity and Infrastructure Security Agency, the importance of sustaining and modernizing authorities for public-private coordination, and the need for greater visibility and coherence in the Information and Communications Technology and Services (ICTS) supply chain.

Our Partnership with the Cybersecurity and Infrastructure Security Agency

The communications sector maintains a strong and longstanding partnership with Cybersecurity and Infrastructure Security Agency (CISA), the federal government's lead civilian agency for cybersecurity and critical infrastructure coordination. This collaboration reflects a broader tradition of partnership between the telecommunications industry and the U.S. government that spans over six decades. That spirit of collaboration continues today as USTelecom and its members work closely with partners across the federal government to strengthen the security and resilience of America's communications infrastructure.

As cyber threats grow more sophisticated and interconnected, today's adversaries increasingly target entire digital ecosystems rather than isolated networks or individual points of failure, exploiting the complexity and interdependence of modern infrastructure to gain persistent access into critical systems. In this environment, resilience can no longer be fragmented or reactive. Meeting these evolving threats requires collaboration that is agile, operationally coordinated, and deeply integrated across government and industry, supported by strong public-private

partnerships and cross-sector coordination already taking place across the critical infrastructure community.

One of the strongest examples of this collaborative model in practice is the President's National Security Telecommunications Advisory Committee, which has been a force multiplier for communications security because it puts industry expertise directly into national decision-making. Instead of disconnected policy, it produces recommendations grounded in how networks actually operate, which leads to smarter resilience planning and more realistic security standards. That connection has helped ensure that when crises hit—whether cyber or physical—communications systems are better prepared to stay online and recover quickly.

This model of operational collaboration has also proven highly effective through initiatives such as the Enduring Security Framework which has strengthened the sector by giving companies access to high-level threat insight they wouldn't otherwise have. That intelligence, combined with direct collaboration with government experts, has led to stronger protections around key technologies like 5G and supply chains. We believe the Enduring Security Framework, in particular, deserves to be continued and supported as CISA advances its mission in partnership with industry.

To meet this moment, we must build on what has already proven effective: deep public-private collaboration, including our longstanding partnership with CISA, while modernizing the foundations that support resilient cybersecurity and secure technological innovation. That means investing not only in advanced tools and capabilities, but also in the digital and physical infrastructure needed to support secure AI deployment across critical sectors. Central to that foundation is connectivity. Streamlined and predictable permitting processes are essential to accelerate broadband deployment, particularly in rural and underserved communities. Expanding high-speed connectivity is not just an economic priority; it is a national security imperative. Without resilient, ubiquitous broadband infrastructure, the benefits of AI-driven defense capabilities and next-generation cryptography cannot be realized at scale, leaving vulnerabilities that adversaries can exploit.

Equally important is modernizing broadband networks. Continued investment in next-generation infrastructure—such as fiber deployment—enhances both the performance and security of communications networks. Modern networks are inherently more adaptable, allowing providers to deploy security updates more quickly, segment and manage traffic more effectively, and integrate advanced protections directly into network operations. These capabilities improve overall resilience, support rapid threat detection and response, and ensure that communications infrastructure can evolve alongside emerging technologies like AI and quantum-resistant encryption.

CISA's role as an enabler of the public-private partnership is essential. As a convener with cross-sector visibility, CISA supports information sharing, facilitates collaboration, and helps align efforts across government and industry. A key component of this partnership is the legal framework that supports information sharing. The long-term reauthorization of the Cybersecurity Information Sharing Act of 2015 is therefore critical. This statute provides the foundation for

trusted, voluntary sharing of cyber threat information and underpins many of the collaborative efforts that exist today.

But resilience cannot stop at the federal level. USTelecom also supports Chairman Ogle's bipartisan PILLAR Act to reauthorize CISA's State and Local Cybersecurity Grant Program, which extends CISA's collaborative model beyond the federal level by strengthening cybersecurity capabilities across state, local, tribal, and territorial governments. By providing resources to enhance planning, coordination, and resilience, the program helps ensure a more consistent and aligned approach to cybersecurity across the broader ecosystem that communications networks rely on.

The challenges facing our digital infrastructure are no longer confined to any single network, company, or sector. Defending against increasingly sophisticated threats requires sustainable partnerships and a shared understanding of how critical systems function in the real world. The collaboration between CISA and the communications sector has helped build that foundation and strengthening it will be essential to ensuring that the infrastructure connecting and securing the nation remains resilient in the face of rapidly evolving threats.

Sustaining and Modernizing Public-Private Coordination Authorities

The United States benefits from a long-standing tradition of public-private collaboration in securing critical infrastructure. That collaboration is not incidental; it is built on legal authorities, institutional frameworks, and mission-driven relationships that have developed over time. As the threat environment becomes more dynamic and interconnected, there is a need to ensure that these authorities remain fit for purpose. Mechanisms for collaboration must be able to support not only strategic dialogue, but also timely, operational engagement.

Existing frameworks—such as those historically supported through advisory structures like the Critical Infrastructure Partnership Advisory Council—have demonstrated the value of providing a trusted environment for government and industry to share information and coordinate on security challenges. At the same time, the pace and complexity of today's threat landscape call for capabilities that are more persistent, more agile, and more directly aligned with operational needs.

To that end, there is a clear opportunity to build on these foundations by modernizing how coordination occurs. One approach is the development of a standing capability—referred to conceptually as the Alliance of National Councils for Homeland Operational Resilience, or "ANCHOR"—that would support continuous engagement between government and industry on cybersecurity and resilience.

Such a capability should move beyond episodic or incident-driven interaction and instead provide a durable framework for collaboration. It should enable real-time information exchange, joint planning, and coordinated response, while also supporting longer-term efforts to identify and mitigate systemic risk.

Importantly, this type of modernization should not be about creating new layers of bureaucracy. It should be about ensuring that existing authorities and partnerships are structured in a way that reflects current operational realities. CISA is the appropriate entity to support this kind of effort. Its existing role, relationships, and experience position it to facilitate sustained collaboration in a manner that is both effective and trusted by industry. Initiatives such as the forthcoming "Critical Infrastructure (CI) Fortify" program, a collaborative effort between CISA and allied partners designed to help critical infrastructure organizations maintain operations during periods of geopolitical conflict, will build on structured collaboration between government and industry.

These efforts show that when operational expertise and coordinated planning come together, they can produce meaningful outcomes on complex cybersecurity challenges. The task before us is to ensure that these partnerships are not episodic responses to emerging threats, but enduring foundations for long-term resilience.

ICTS Supply Chain – The Need for Visibility and Coordination

The security of the Information and Communications Technology and Services supply chain is a critical priority for the communications sector and for the nation as a whole.

Over the past several years, there has been significant bipartisan interest in addressing risks associated with the ICTS supply chain. Congress and successive Administrations have taken important steps to respond to cyber and geopolitical challenges, including those associated with the People's Republic of China. These efforts reflect serious and legitimate national security concerns.

At the same time, these initiatives have developed across multiple agencies and authorities, often in parallel rather than in coordination. Today, several parts of the federal government assert jurisdiction over different aspects of the ICTS ecosystem, including the Department of Commerce's Bureau of Industry and Security, the Federal Communications Commission, the Federal Acquisition Security Council, the Federal Acquisition Regulation Council, and the Department of War, alongside various congressional directives.

While each of these efforts is grounded in valid objectives, the cumulative effect is a regulatory environment that can be fragmented and, at times, difficult to navigate. This fragmentation presents a number of practical challenges. In some cases, there are overlapping or unclear lines of jurisdiction, where similar technologies, services, or entities may be evaluated under different authorities and standards. There are also instances where determinations affecting ICTS products or services are not accompanied by sufficient transparency. Without clear explanations, it can be difficult for companies to understand the basis for decisions or to take appropriate steps to mitigate identified risks.

Operational uncertainty is another concern. Changes in how equipment, companies, or transactions are treated—particularly when those changes are not uniform across agencies—can disrupt planning, investment, and supply chain decisions. This is especially significant in a sector where infrastructure investments are long-term and capital-intensive.

In addition, companies are often required to navigate a complex set of compliance obligations that may not be fully aligned. This increases costs and administrative burdens, and it can complicate efforts to maintain secure and resilient supply chains. These challenges have real consequences. They can slow the deployment of secure technologies, create inefficiencies, and, in some cases, make it more difficult to achieve the underlying national security objectives.

Greater visibility into ICTS-related risks, combined with more consistent coordination across agencies, would help address these issues. Industry benefits from timely, actionable information that supports effective risk management and informed decision-making.

Congress can play an important role in encouraging continued interagency coordination, promoting consistency in implementation, and supporting greater transparency in how ICTS-related risks are identified and managed. Aligning existing authorities—rather than adding new, overlapping requirements—will help ensure that security objectives are achieved in a manner that is predictable, effective, and sustainable.

Conclusion

In closing, the increasing interconnection of communications and information technology systems requires a governance approach that emphasizes coordination, clarity, and partnership. Our experience demonstrates that when government and industry work together within a clear and durable framework, we can effectively address complex and evolving threats. Strengthening our partnership with CISA, modernizing the authorities that support public-private collaboration, and improving coordination in the ICTS supply chain will help ensure that the United States remains secure and resilient.

Thank you for the opportunity to testify. I look forward to your questions.

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:

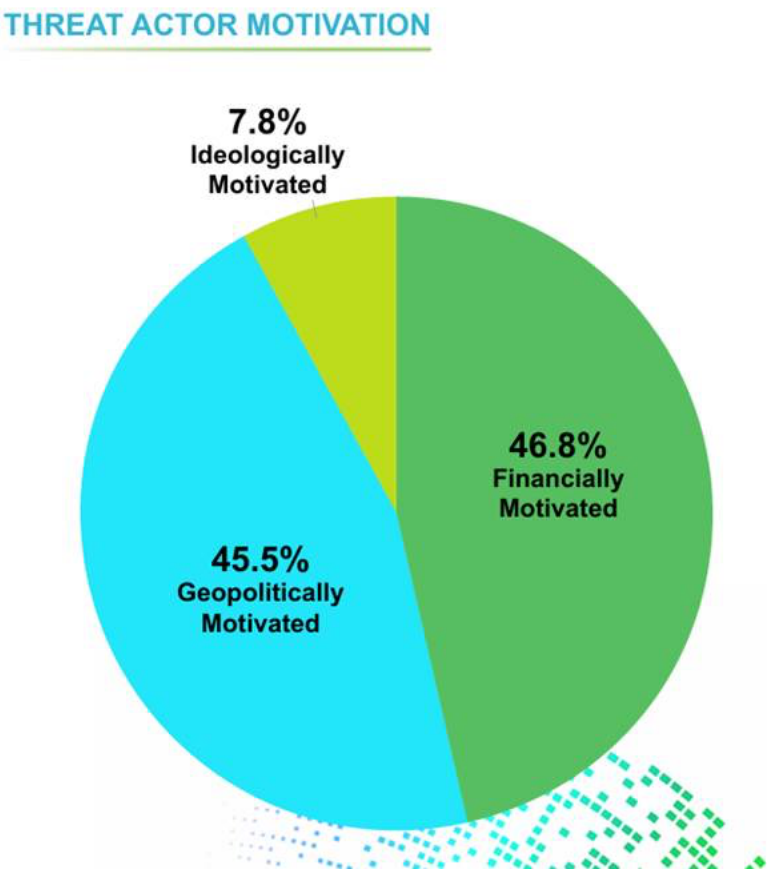
- Access to 330+ Adversary Attack Playbooks mapped to the MITRE ATT&CK® Framework, enabling members to share and learn tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs).
- Ransomware Tracker that contains 15,000+ reported ransomware incidents, including those specific to 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

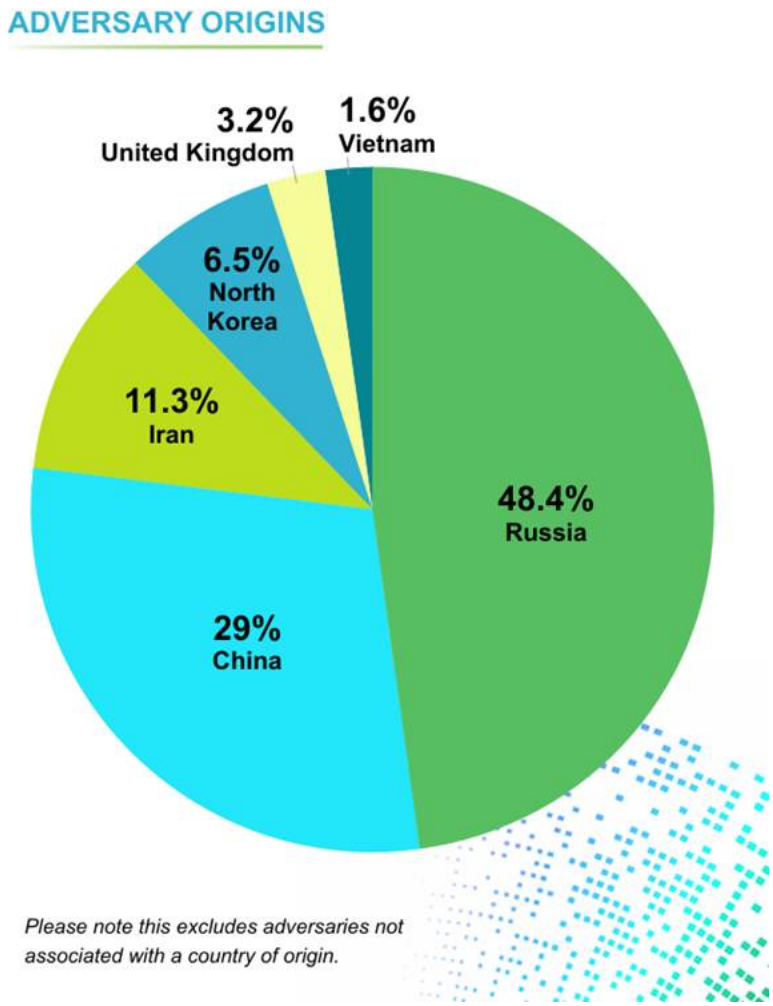
The country faces an unprecedented array of cyber risks. Networks are interconnected across the globe. The pace of technological change is exploding. Corporate budgets are constrained. Threat actors are collaborative, highly skilled, and well-financed. In fact, the economics favor the attackers. It is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



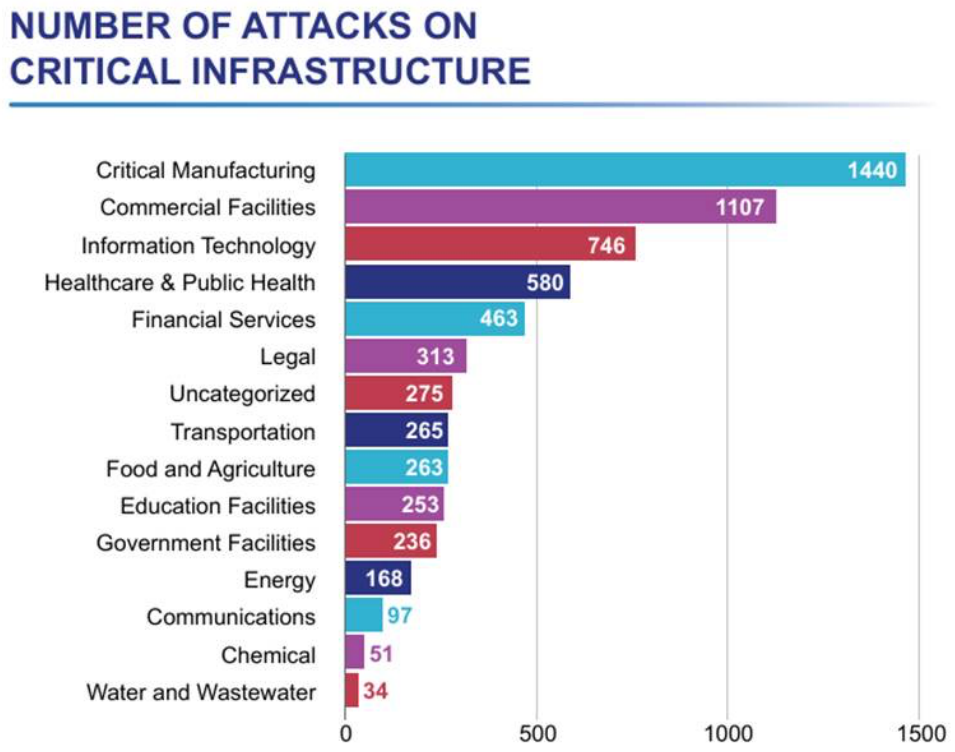
Iran is highly capable in the cyber domain. About 11% of observed threat actors active in the sector are based in Iran. Although the line between a nation-state actor and an affiliate actor can be blurry, Iran hosts a range of actors who operate with the blessing of the Iranian authorities. These threat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