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)