BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

June 24, 2025

Mr. Chip Pickering
Chief Executive Officer
INCOMPAS
1100 G Street NW, Suite 800
Washington, DC 20005

Dear Mr. Pickering,

Thank you for appearing before the Subcommittee on Communications and Technology on Wednesday, June 4, 2025, to testify at the hearing entitled, "AI in the Everyday: Current Applications and Future Frontiers in Communications and Technology."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Tuesday, July 8, 2025. Your responses should be mailed to Noah Jackson, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to noah.jackson@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Richard Hudson
Chairman
Subcommittee on Communications and Technology

CC: The Honorable Doris Matsui, Ranking Member, Subcommittee on Communications and Technology

Attachment —Additional Questions for the Record

The Honorable Russ Fulcher

1. **The Salt Typhoon attack was done by Chinese cyberattackers who found "known vulnerabilities in access points" to get into communications networks and then collect user calls and text messages, along with IP addresses – including of presidential and vice-presidential candidates. How can Generative AI be scaled to detect malware seeking to infiltrate communications networks in entities like data centers where large amounts of data flow through the networks?**

Response:

The application of generative AI in cybersecurity is an area of growing interest and INCOMPAS urges Congress to enable industry to continue research, testing, and collaboration to ensure these models' effectiveness as well as our nation's security. In environments like data centers, generative AI may support early detection of novel threats by augmenting traditional cybersecurity tools with real-time analysis. In many cases, data center operators are already using generative AI models to monitor and analyze data and detect threats in real time by comparing observed data to what it has modeled as normal user or system behavior. These models can then identify anomalies that deviate from expected behavior, alerting the operator to potential threats.

Several U.S.-based companies are leading the way in utilizing generative AI to enhance cybersecurity threat detection and mitigation, including several INCOMPAS members. For example, through its Mandiant and Chronicle platforms, Google Cloud is using large language models (LLMs) to enhance threat intelligence and automate the detection of malware across global data flows. *See* Blog, *Introducing AI-powered insights in Threat Intelligence*, GOOGLE CLOUD (Apr. 24, 2023) *available at* https://cloud.google.com/blog/products/identity-security/rsa-introducing-ai-powered-insights-threat-intelligence. Microsoft Security CoPilot is another commercially available generative AI model that operators are using to assist in threat analysis. *See Microsoft Security Copilot*, MICROSOFT, *available at* https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot.

2. **Thank you for noting policies like "right of way" when it comes to fiber networks and the larger broadband efforts in rural areas. I have legislation to make progress on that, given our large federal footprint, and I appreciate the care local broadband providers take. One thing I have heard from small Internet Service Providers that I raised in a previous hearing is the fact that they have extensive cybersecurity incident reporting requirements that are not always standardized or consistent across federal agencies. Can you provide any insights or suggestions on ways to harmonize the reporting, or perhaps sharing reporting of cybersecurity incidents between CISA and agencies like the FCC, along with that needed by the FBI, Secret Service, and related federal, state, and local law enforcement?**

Response:

INCOMPAS and its members are committed to working with Congress and federal agencies to support a nationwide, coordinated, risk-based approach to cybersecurity that enhances national resilience while minimizing unnecessary burdens on providers. The Trump administration has taken steps to improve interagency coordination and streamline cybersecurity reporting requirements. The June 2025 Executive Order on "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity" directs agencies to adopt interoperable cybersecurity standards and enhance collaboration on threat detection and response. As part of this collaboration, INCOMPAS would urge the administration to direct federal, state, and local agencies to develop a common cybersecurity incident reporting portal that could be accessed by agencies of jurisdiction. Such a portal would harmonize incident reporting while still giving agencies the ability to seek additional information if necessary.

Additionally, the March 2025 Executive Order on "Achieving Efficiency Through State and Local Preparedness" calls for a unified National Resilience Strategy, which includes aligning federal cybersecurity efforts with those of states and localities. INCOMPAS believes these are positive steps toward achieving greater coordination across government entities, including CISA, the FCC, the FBI, the Secret Service, and state and local law enforcement, as we support efforts that reduce duplication, improve information sharing, and strengthen our national cybersecurity.

3. **I have been reading about "Discriminative AI" that doesn't just recognize patterns in large amounts of data but can also detect anomalies and help operators to take evasive action such as cutting off some parts of the communications stream to stop it from infecting the entire network. It can also help operators set predictive criteria for detection of such malware. Can you expound upon these capabilities? How are you working with network communications infrastructure players to integrate these abilities to help them strengthen their detection abilities? Can you tell me about the partnerships that are developing from these in the industry?**

Response:

Discriminative AI models are designed to detect anomalies in large datasets and may support cybersecurity detection by identifying unusual patterns that could indicate malware or other threats. These capabilities can assist service providers in taking proactive measures, such as isolating parts of a network or applying predictive criteria to flag suspicious activity. Many in the communications and technology industries are exploring the use of advanced AI tools to improve threat detection and response. One example of an INCOMPAS member that integrates threat detection capabilities into its network products is Google Cloud. Google Cloud has partnered with cybersecurity firm **Fortinet** to enhance real-time threat detection for telecom providers. Using Google's **Vertex AI** and Fortinet's security tools, this collaboration helps telecoms identify and respond to threats more quickly and effectively. Google Cloud Telecom AI Partnerships

Another example of the use of Discriminative AI in threat detection is in the robocall mitigation ecosystem. Our members and their third-party partners are using AI algorithms to identify patterns and distinguish legitimate calls from spam. As these algorithms are fine-tuned, carriers are able to reduce instances of false positives and flag robocalls more effectively, ultimately keeping consumers safe and protecting them from fraud.

Many of our companies are evaluating partnerships and pilot programs in this area, including the FCC's Cybersecurity Pilot Program for schools and libraries, which includes AI/ML threat detection and response among its list of eligible equipment and services. INCOMPAS supports

continued dialogue across industry and government to better understand how emerging technologies like Discriminative AI can contribute to a more secure communications ecosystem.

The Honorable August Pfluger

1. I am highly concerned about the national security implications of foreign-owned data centers in the United States. Such ownership would provide adversaries with direct access to Americans' sensitive personal data, allow for the disruption of critical infrastructure, or increase the risk of espionage or misuse for malicious purposes. Do you see potential risks posed by foreign adversary-owned or influenced companies from building data centers in the United States?

Response:

INCOMPAS recognizes the importance of ensuring that data centers operating in the United States uphold the highest standards of cybersecurity, transparency, and operational integrity, regardless of ownership. While concerns about foreign influence are understandable, particularly in the context of adversarial nation-state activity, it is also important to focus on the security practices, regulatory compliance, and operational accountability of any entity operating critical infrastructure.

There are strong examples of American-owned and operated data center companies, such as INCOMPAS member DC BLOX, which is investing in secure, resilient infrastructure across the Southeast and working closely with public and private partners to meet national security expectations. DC BLOX demonstrates how domestic leadership in the data center space can contribute to both economic growth and national resilience.

American owned data centers have a significant positive impact on the local communities where they are located, bringing jobs, investment, tax dollars, and philanthropy. They provide employment opportunities for residents and stimulate economic growth. The opportunities for construction jobs include hiring local, skilled trades labor, while operational jobs, many of which do not require a 4-year degree, include a diversity of positions, such as technicians, heating and cooling specialists, engineers, project managers, site managers and more. Also, the investment in data centers also brings significant tax dollars to the community, funding important public services including local public schools and infrastructure projects. Lastly, data centers require robust local infrastructure such as the expansion and upgrades of local roads, power infrastructure, network speeds, and water systems. This benefits residents and drives even more economic development for communities.

Foreign-owned data centers need to be held to the same standards and expectations. INCOMPAS supports transparent and enforceable cybersecurity standards applied consistently across the sector as key to protecting sensitive data and critical systems. We support continued dialogue between industry and government to ensure that all operators, regardless of origin, are held to the same high standards of trust and accountability.

2. **From my understanding, the majority of components used in data centers, which AI systems rely on, have complex global supply chains. Many critical parts are manufactured or assembled in foreign countries, sometimes by companies with ties to adversarial governments. This raises additional concerns about the potential for hardware backdoors or hidden vulnerabilities to be intentionally embedded during manufacturing, which could be exploited to compromise U.S. data security or disrupt**

critical operations. Given these risks, do you have concerns about the national security implications of relying on AI components or hardware sourced from foreign adversaries, particularly regarding the possibility of supply chain tampering or embedded backdoors?

Response:

INCOMPAS and our membership remain committed to strengthening national security and increasing the domestic workforce and manufacturing of components of AI Infrastructure. When it comes to securing AI components, INCOMPAS members have implemented a "zero trust" mentality, with multiple layers of security (physical and cyber), strict protocols, and checks and balances with which every person handling data or hardware must comply. Hardware, such as data storage devices, has a strict chain of custody to ensure there was no supply chain tampering. Hardware devices are destroyed onsite at the end of their life to ensure data breaches do not occur.

At the same time, our country must increase both manufacturing facilities and the workforce needed to domestically produce the hardware components of AI infrastructure needed to keep with demand and maintain our position in the AI race. INCOMPAS urges Congress to take the necessary steps to support this manufacturing, which will spur economic growth and secure our country's AI future.

Also, the U.S. needs to create a myriad of opportunities and programs to develop a new generation of workers. Congress should work with relevant government agencies to study workforce impact across different industries over time. These parties should work together to determine which new jobs will likely be created by AI and other emerging technologies. Such analyses can help determine specific education and upskilling policies based on need. Some can focus on community and vocational schools while other programs can be regionally focused, addressing the specific needs of a region.

3. **Are there regulatory or enforcement gaps that could allow foreign adversaries to gain control or influence over our data infrastructure?**

Response:

INCOMPAS recognizes the importance of protecting communications networks from undue foreign influence. We agree that ensuring the integrity of data infrastructure requires a coordinated, risk-based approach. The U.S. government has established mechanisms to assess national security risks associated with foreign involvement in communications infrastructure. Team Telecom is an interagency group led by the Department of Justice, with participation from the Departments of Homeland Security and Defense. Team Telecom reviews foreign ownership and investment in telecommunications infrastructure and advises the FCC on potential national security and law enforcement concerns. INCOMPAS believes that strong, transparent, and consistently enforced cybersecurity standards applied across all operators are essential to protecting critical infrastructure. Continued collaboration between industry and government remains crucial to identifying any potential regulatory or enforcement gaps and ensuring that all entities operating in the U.S. communications ecosystem adhere to the highest standards of accountability and security.

4. **Would new legislative measures - such as a ban on foreign adversary control over data centers and critical components - be necessary to close these gaps and ensure robust protection?**

Response:

INCOMPAS shares the concern about foreign-adversary influence over critical infrastructure. We believe the most effective path forward today lies in Congress developing a comprehensive national AI infrastructure and cybersecurity policy framework as I discussed during the hearing. This approach should emphasize strong cross-government coordination, robust cybersecurity protocols, transparency and accountability in ownership and control of infrastructure, and streamlined permitting requirements for AI corridors and connectors, data centers, and energy to facilitate deployment of U.S.-based networks. Such a framework will provide the flexibility and resilience needed to address evolving threats while preserving innovation and investment in our digital economy.

5. **I also recognize the importance of maintaining U.S. leadership in technology and innovation. Mr. Pickering, what potential economic or innovation impacts should Congress consider when restricting foreign investment and participation in our data center and AI supply chains?**

Response:

Restricting foreign investment in AI and data center infrastructure must be balanced with policies that accelerate domestic production and innovation. Increasing U.S.-based manufacturing of critical components, including fiber and energy technologies, is essential to reducing supply chain vulnerabilities and creating high-quality jobs. INCOMPAS commends the Department of Energy and NTIA for their joint initiative to build data centers on federal lands and expand domestic data center capacity, which strengthens both our innovation ecosystem and national security. Continued investment in energy-efficient, sustainable infrastructure will help ensure the U.S. remains the global leader in AI. At INCOMPAS, we believe fostering open, competitive markets alongside targeted strategic safeguards is the key to long-term economic growth and technological leadership.

6. **How can we balance national security with continued technological advancement and global competitiveness?**

Response:

To effectively balance national security with continued technological advancement and global competitiveness, the U.S. must adopt a strategic, coordinated policy approach. INCOMPAS strongly supports the development of a comprehensive national policy framework for AI that reinforces both U.S. security and economic leadership.

Policymakers play a critical role in fostering a "whole of government" approach to AI and cybersecurity that ensures robust coordination across federal agencies. This coordination is essential to provide the private sector with the clarity and consistency it needs to innovate securely and confidently. Fragmented or conflicting requirements only hamper progress and weaken our national posture.

A forward-looking national security strategy must also prioritize investments in education and workforce development. Building a skilled, AI-proficient workforce is essential to maintaining our competitive edge and ensuring long-term resilience. By establishing a consistent, national approach to security, we can reduce vulnerabilities, streamline compliance for businesses, and create an environment that fosters healthy competition and sustains innovation.