



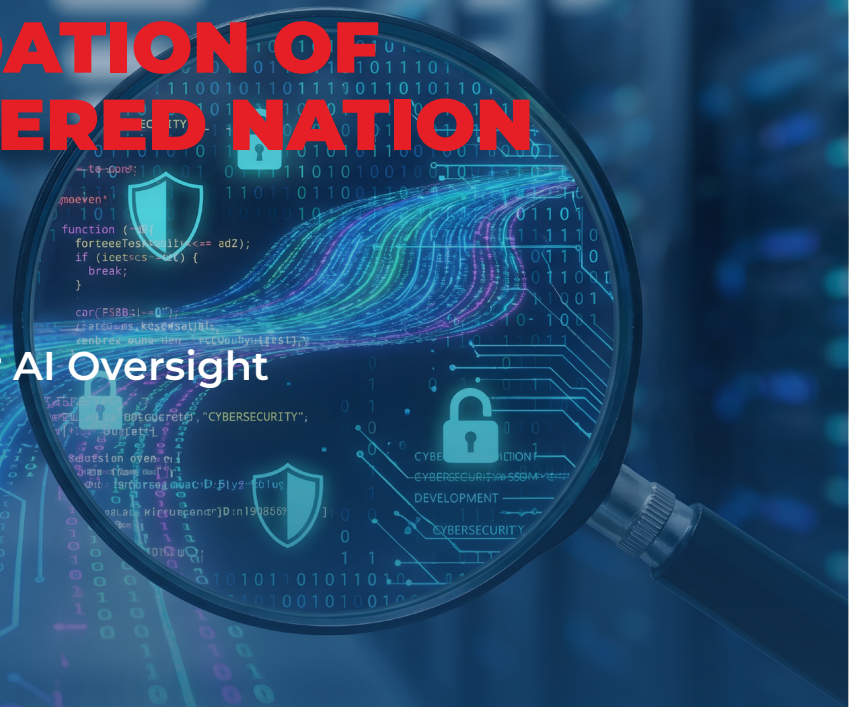
THE RESILIENCE IMPERATIVE:

SECURING COMMUNICATIONS INFRASTRUCTURE AS THE FOUNDATION OF AN AI-POWERED NATION

AUTHORS:

Brian Allen, Center for AI Oversight

Mike Regan, TIA





INTRODUCTION

For more than a century, the communications sector has served as the central nervous system of national infrastructure, enabling economic activity, public safety, and global connectivity. In the analog era, the industry engineered networks capable of physical resilience under harsh environmental conditions. In the software-defined era, it developed cyber-resilience frameworks to counteract escalating digital threats. Today, as the United States enters the cognitive era, defined by the widespread integration of artificial intelligence (“AI”) across critical systems, the sector must elevate its resilience posture once again. Communications networks—and the global supply chains that underpin them—have become foundational to the functioning, security, and reliability of autonomous systems, national defense, critical infrastructure, and the emerging AI economy.¹

AI-enabled systems place unprecedented demands on communications networks. Next-generation data centers—densely packed with graphics processing units (“GPUs”), tensor processing units (“TPUs”), and specialized AI accelerators—now require high-performance, low-latency, and continuously available network connectivity from end to end.² These facilities function as cognitive epicenters that

drive workloads for autonomous vehicles, robotics, logistics, energy grids, financial services, and public-sector operations, systems the World Economic Forum notes are increasingly dependent on high-quality data, connectivity, and digital infrastructure.³ The communications network has thus evolved into a converged, interdependent infrastructure, linking hyperscale AI compute centers with edge devices and mission-critical applications. As governmental studies have noted, while 5G and future 6G networks introduce capabilities essential to national competitiveness, they also expand the risk surface for cyberattacks, supply chain infiltration, and cascading failures.⁴

This environment presents a dual reality: the risks are greater, but so are the opportunities. In a world where AI-driven services will depend on verifiable trust, communications providers capable of demonstrating provable integrity, supply chain security, and resilience will become indispensable to both government and industry.⁵ Standards-based assurance, transparent and trustworthy supply chains, and governance models that establish “trustworthiness by design” will define leadership in the next decade.

COMMUNICATIONS NETWORKS' EXPANDING RESPONSIBILITY IN THE AI ERA

THE RE-ARCHITECTURE OF NETWORKS UNDER AI LOAD

The AI-driven transformation of digital infrastructure requires a fundamental re-architecture of communications networks. Driven by densely clustered AI accelerators, data center rack power densities have surged far beyond the historical 5–10 kW average, with high-density workloads now pushing individual racks from 25 kW to well over 100 kW.⁶ While this dramatic increase is dominated by the GPUs themselves, this extreme concentration of compute power creates a critical secondary challenge for the network. The supporting network fabric must evolve to handle the massive data flows and thermal loads, and in doing so, it becomes a significant and growing contributor to the data center's overall power consumption. This power-dense environment requires corresponding increases in fiber capacity, network efficiency, and adaptive routing, as the AI sector is estimated to consume a significant and rapidly growing portion of global data center power by 2026.⁷

Modern 5G/6G and optical transport layers are increasingly software-defined, leveraging AI-enabled orchestration tools for load balancing, network slicing, automated anomaly detection, and resource allocation.⁸ Next-generation AI-based controllers are designed to dynamically reconfigure radio access networks ("RAN"), optimize fronthaul and backhaul performance, and respond autonomously to outages or cyber anomalies.⁹ The reliability of these AI-enabled network functions depends on the integrity and security of the underlying hardware, software, and training data.

NATIONAL SECURITY DIMENSIONS

Communications infrastructure has long been recognized as critical national infrastructure. In the AI era, however, this dependency introduces acute geopolitical risks. These concerns are not theoretical but are a direct response to active threats. The state-sponsored actor Volt Typhoon, for example, has been identified by U.S. intelligence agencies as a PRC-backed group that has successfully infiltrated U.S. critical infrastructure, with a specific focus on the communications sector. Their documented objective is to pre-position themselves for future disruptive or destructive cyberattacks during a potential geopolitical crisis, aiming to sever connectivity and sow chaos.¹⁰

This real-world strategy of pre-positioning latent threats validates the U.S. government's heightened focus on safeguarding AI and 5G/6G-enabled infrastructure from malicious foreign interference and untrusted vendors, as emphasized in recent executive orders.¹¹ Congressional actions, such as the Secure Equipment Act of 2021, further reflect these persistent concerns about adversarial infiltration through opaque or high-risk foreign suppliers.¹²

The integrity of the communications supply chain is therefore a national security priority of the highest order. Where earlier generations of networks relied on monolithic equipment, today's disaggregated, software-defined environments involve hundreds of suppliers, open-source components, and cloud orchestration systems.¹³ Without verifiable standards and transparent supply-chain governance, this vast and complex attack surface becomes both opaque and unmanageable.

HIGH-IMPACT THREAT SCENARIO: THE AUTONOMOUS CASCADE FAILURE

To illustrate the national-level implications of supply chain compromise in the AI era, consider a hypothetical “cascade failure” scenario informed by real-world attack patterns.

A malicious actor compromises a specialized AI accelerator chip at the manufacturing stage by embedding a hardware trojan.¹⁴ This component is later installed in a hyperscale data center that hosts AI-driven network-management software responsible for dynamic traffic prioritization across a 6G network. Through the hardware trojan, the adversary manipulates the AI model by injecting poisoned training data, teaching the system to misclassify specific traffic patterns originating from autonomous trucking fleets during emergency conditions.

During a major regional grid failure, the attacker triggers the latent backdoor, activating the malicious classification rule. The AI-network controller autonomously de-prioritizes traffic from the autonomous trucking fleet, causing

widespread loss of connectivity. Autonomous vehicles lose situational awareness, leading to a multi-vehicle pileup. First-responder communications degrade due to the same corrupted network logic. The incident disrupts national supply routes, triggers a federal investigation into communications resilience, and undermines public trust in autonomous systems.

This scenario, while hypothetical, aligns with known threat vectors substantiated by real incidents. The SolarWinds compromise demonstrated how attackers infiltrated tens of thousands of downstream systems by exploiting a trusted software update.¹⁵ The Log4j vulnerability revealed how a single open-source dependency could expose a vast number of critical systems globally.¹⁶ The Kaseya ransomware attack illustrated how compromising a single managed service provider could cascade into thousands of endpoints.¹⁷ Academic research further confirms the feasibility of AI model backdooring, where models behave normally until triggered by specific inputs.¹⁸ The lesson is clear: the convergence of telecom and AI infrastructure transforms supply chain attacks into real-world physical risks, with consequences spanning transportation, public safety, economic stability, and national security.



THE UNSEEN RISK: SECURING THE CONVERGED AI SUPPLY CHAIN

HARDWARE INTEGRITY

AI-enabled communications networks rely on globally distributed manufacturing processes. Hardware components pass through complex supply chains involving design firms, fabrication plants, logistics providers, integrators, and distributors. Each step introduces potential for tampering, counterfeit substitution, or firmware manipulation.¹⁹ Government assessments have highlighted the increasing sophistication of hardware trojans and the difficulty of detecting them once embedded.²⁰

SOFTWARE AND OPEN-SOURCE DEPENDENCIES

Software supply chain risk is now one of the most significant systemic threats to critical infrastructure security. Modern telecom systems use tens of thousands of third-party software libraries, including open-source components.²¹ Public repositories such as PyPI and NPM have documented numerous cases of malicious package uploads designed to infect downstream systems.²² A 2024 security report found that malicious code and vulnerabilities are prevalent in publicly available AI models on platforms like Hugging Face.²³

1 in 10 AI Models Potentially Unsafe

A 2024 security analysis of the public Hugging Face AI model repository found that roughly 10% of the scanned models contained potentially malicious or unsafe code, often through the insecure “pickle” serialization format. This highlights the new and unvetted attack surface introduced by pre-trained AI models.

96% of Code is Not Your Own

For the average enterprise software application, open-source dependencies make up as much as 96% of the codebase. This vast, interconnected web of third-party code means a single vulnerability in a popular library can create a systemic, global risk, as demonstrated by the Log4j incident.

INTERNAL PROCESS AND INSIDER RISKS

Beyond external suppliers, a significant risk surface exists within the organization itself, stemming from both malicious insiders and, more commonly, unintentional security lapses. A privileged developer, for instance, could intentionally insert a backdoor into a proprietary AI model or, through a simple error, introduce a critical vulnerability by pulling an unvetted open-source package into a production build. More fundamentally, these individual points of failure become systemic risks in the absence of a robust Secure Software Development Framework (SSDF). Without mandatory controls for code integrity, vulnerability scanning, and access management, the development pipeline itself becomes the most dangerous link in the supply chain, allowing an adversary to compromise the software or AI models being delivered to customers.²⁴

THIRD-PARTY AND “AS-A-SERVICE” RISKS

Communications providers increasingly outsource analytics, orchestration tools, cloud functions, and AI services to third-party vendors. This interdependence creates near-fractal risk propagation: compromise of a cloud service, managed service provider, or AI platform can impact multiple telecom operators simultaneously, a risk highlighted in analyses of systemic technology dependencies.²⁵

NEED FOR VERIFIABLE PROOF

Traditional vendor self-attestations cannot provide meaningful assurance in this environment. Foundational guidance from NIST’s Cybersecurity Supply Chain Risk Management Framework emphasizes the need for verifiable controls and transparency across all tiers of the supply chain.²⁶ This is further specified by the NIST AI Risk Management Framework, which calls for practices to ensure the trustworthiness of AI systems,

including the integrity of models and the data they are trained on throughout their lifecycle.²⁷ The emerging consensus across government, industry analysts, and standards bodies is that trust must be earned, proven, and continuously monitored—not assumed.

A FRAMEWORK FOR NATIONAL RESILIENCE AND MARKET LEADERSHIP

THE ROLE OF STANDARDS IN SECURING INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SUPPLY CHAINS

A global consensus is emerging that foundational frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001, while essential, are insufficient to address the unique risks of AI-era communications.²⁸ This shift is evident in new, targeted regulations and standards. In the European Union, the AI Act imposes legally binding requirements on data and model integrity for high-risk systems, while the Cyber Resilience Act mandates secure-by-design principles for all products with digital elements.²⁹ These regulations mirror the principles outlined in the NIST AI RMF and C-SCRM frameworks, moving them from voluntary guidance to market-entry requirements.

In response, international standards bodies have developed certifiable, process-based frameworks. Standards such as ISO/IEC 42001 provide a globally recognized structure for managing AI risks, while industry-specific standards are needed to verify the integrity of the underlying ICT supply chain.³⁰

TIA'S SCS 9001 STANDARD

The Telecommunications Industry Association (“TIA”) developed SCS 9001, the world’s first certifiable ICT supply chain security standard, to address this need.³¹ SCS 9001 provides verifiable requirements for supplier vetting, secure development practices, component traceability, tamper-evident logistics, and incident response governance. The standard operationalizes

federal supply chain guidance and enables organizations to demonstrate compliance through independent audits rather than self-attestation.

BENEFITS OF A STANDARDS- BASED APPROACH

Adopting a standards-based approach to supply chain security is more than a defensive measure; it is a strategic asset that delivers distinct advantages in three key areas:

- **Operational Resilience and Trust.**
A standards-based approach strengthens resilience by complementing vendor commitments with provable assurance. Verifiable controls for hardware, software, and AI models reduce the risk of catastrophic failures from hidden threats. A single supply chain compromise can cause nationwide outages and irreparable harm to a brand. In this high-stakes environment, verifiable integrity becomes the bedrock of customer trust and service reliability.³²
- **Competitive Advantage and Market Access.**
Demonstrable security is a powerful competitive differentiator. Government contracts and high-value enterprise clients in finance and healthcare now demand proof of supply chain integrity. Providers with a certified secure supply chain can meet requirements that their competitors cannot. This transforms a security investment into a powerful tool for winning business and capturing market share in the most lucrative sectors.³³
- **Shaping Policy and Reducing Liability**
Proactive adoption of rigorous standards allows providers to define the future of security regulation, not just react to it. This approach provides tangible evidence of due diligence, creating a strong, more defensible position against potential litigation and helping satisfy the critical board-level duty of care established by legal precedents like *In re Caremark*.³⁴ It also allows the industry to present regulators with a workable, effective model for security, preempting less practical government mandates.

VI. UPDATED AI/ML THREAT MATRIX

(Table presented in simplified academic text format for clarity.)

Category	Threat Examples
Component Integrity	Hardware tampering; chip-level trojans; counterfeit component substitution; firmware-level backdoors. Model provenance failures; tampered pre-trained models.
Third-Party Dependencies	Open-source package poisoning; library hijacking; malicious model repositories. SBOM manipulation or incompleteness.
Data Security and Integrity	Data poisoning attacks; training data corruption; membership inference; inadvertent memorization of PII. Data drift and label integrity failures.
Model Security	Backdoored models; adversarial examples; model extraction attacks; IP theft.
DevSecOps/MLOps	Compromised CI/CD pipelines; malicious model updates; weak signing and verification practices.
Governance & Strategy	Lack of a formal AI risk management framework; unclear lines of responsibility. Outdated security policies that fail to govern the entire AI lifecycle, leading to an inability to keep pace with emerging threats and opportunities.
Workforce & Skills Gap	Shortage of personnel with combined expertise in AI and cybersecurity; inability to identify and mitigate novel AI-specific attack vectors. Untrained developers introducing vulnerabilities into models or MLOps pipelines.

VII. CONCLUSION: A CALL TO LEADERSHIP

The integration of artificial intelligence is fundamentally reshaping the communications landscape. As AI becomes embedded across critical sectors, from autonomous transportation to emergency services, the reliability and security of the underlying communications infrastructure will become paramount. The analyses presented here underscore the urgent need for the communications sector to proactively address the specific challenges and opportunities presented by the convergence of AI and network technologies.

The communications industry should prioritize the ongoing evolution of its established frameworks to ensure they remain fit-for-purpose in the AI era. TIA's SCS 9001 standard provides a robust framework for ICT supply chain security. SCS 9001 can be leveraged to explicitly incorporate the unique risks

of the AI supply chain—including model provenance, training data integrity, and the security of specialized accelerator hardware. Adopting SCS 9001 promotes building and demonstrating verifiable trust.

The communications industry stands at an inflection point. The governance models of the past are not fully equipped to meet the demands of a future defined by autonomous systems and AI-dependent critical infrastructure.

We invite you to join us in shaping the future of AI risk management for the ICT industry. Your insights and expertise are critical to developing frameworks that safeguard innovation while upholding security, resilience, and ethical responsibility. Your involvement will help ensure that our industry leads with confidence and integrity in this transformative era.

REFERENCES

- ¹ See, e.g., U.S. Cybersecurity & Infrastructure Security Agency, *ICT Supply Chain Risk Management Task Force: Year 2 Report* (2020).
- ² Int'l Energy Agency, *Electricity 2024: Analysis and Forecast to 2026* (2024).
- ³ See World Econ. F., *The Urban Mobility Scorecard Tool: Benchmarking the Transition to Sustainable Urban Mobility* (2024).
- ⁴ See U.S. Gov't Accountability Office, GAO-21-26SP, *5G Wireless: Capabilities and Challenges for an Evolving Network* (2020).
- ⁵ See World Econ. F., *Global Cybersecurity Outlook 2023* (2023).
- ⁶ For general trends, see Int'l Energy Agency, *Electricity 2024: Analysis and Forecast to 2026* (2024). For specific figures on extreme density racks, see also Julius Neudorfer, *Looking Back at Data Center World 2023: 3 Concerns That Stood Out*, Data Ctr. Knowledge (Apr. 28, 2023).
- ⁷ *Id.*
- ⁸ See 3GPP TR 28.809 V17.0.0, *Study on enhancements of Artificial Intelligence (AI)/Machine Learning (ML) for NR network automation* (rel 17) (2022).
- ⁹ *Id.*
- ¹⁰ See U.S. Cyb. Sec. & Infrastructure Sec. Agency, Alert AA24-038A, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* (Feb. 7, 2024).
- ¹¹ See, e.g., Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).
- ¹² Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423.
- ¹³ See generally MITRE, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War* (2022).
- ¹⁴ See, e.g., U.S. Dep't of Def., *Trusted and Assured Microelectronics (T&AM) Program Overview*.
- ¹⁵ See Cybersecurity & Infrastructure Sec. Agency, Alert AA20-352A, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (revised Dec. 30, 2020).
- ¹⁶ See Apache Logging Servs. Project Mgmt. Comm., *Apache Log4j Security Vulnerabilities*, <https://logging.apache.org/log4j/2.x/security.html> (last visited Nov. 17, 2025).
- ¹⁷ See U.S. Cyb. Sec. & Infrastructure Sec. Agency, *CISA-FBI Joint Cybersecurity Advisory: Kaseya VSA Supply-Chain Ransomware Attack (AA21-194A)* (July 2, 2021).
- ¹⁸ See Tianyu Gu et al., *BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain*, in ICLR 2017 Workshop (2017).
- ¹⁹ See U.S. Dep't of Homeland Sec. & U.S. Dep't of Com., *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry* (2023).
- ²⁰ See Nat'l Inst. of Standards & Tech., NISTIR 8517, *Hardware Security Failure Scenarios* (2024).
- ²¹ See Linux Found. Rsch., *The State of Software Bill of Materials (SBOM) and Cybersecurity Readiness* (2023).
- ²² See Sonatype, *The State of the Software Supply Chain* (9th Annual Report 2023).
- ²³ See HiddenLayer, *AI Threat Landscape Report 2024*.
- ²⁴ See Nat'l Inst. of Standards & Tech., SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1* (2022).
- ²⁵ See, e.g., Gartner, *Predicts 2024: The Sourcing, Procurement and Vendor Management Challenge* (2023).
- ²⁶ Nat'l Inst. of Standards & Tech., NIST SP 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022).
- ²⁷ Nat'l Inst. of Standards & Tech., AI 100-1, *Artificial Intelligence Risk Management Framework* (Jan. 2023).
- ²⁸ See ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
- ²⁹ See, e.g., Regulation (EU) 2024/1689 (Artificial Intelligence Act); and Regulation (EU) 2024/2133 (Cyber Resilience Act).
- ³⁰ See ISO/IEC 42001:2023, *Information technology — Artificial intelligence — Management system*.
- ³¹ See Telecommunications Indus. Ass'n, SCS 9001: *The ICT Supply Chain Security Standard*, <https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/> (last visited Nov. 17, 2025).
- ³² See Nat'l Inst. of Standards & Tech., *supra* note 26.
- ³³ See generally Secure Equipment Act of 2021, *supra* note 12.
- ³⁴ See *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

About TIA: The Telecommunications Industry Association (TIA) advances trusted digital infrastructure for a connected world. Representing more than 400 companies globally, TIA brings industry and government together through standards development, government advocacy, certifications, and industry programs to support resilient, innovative infrastructure.

About Center for AI Oversight: The Center for AI Oversight is a 501(c)(3) nonprofit organization advancing the practice of AI oversight governance for boards, executives, and regulators navigating AI adoption.



TO LEARN MORE ABOUT

THE RESILIENCE IMPERATIVE:

CONTACT

TO LEARN MORE ABOUT