PRESIDENTIAL TRANSITION: PRIORITY TOPIC MEMO
JUNE 2024

MITRE | Center for Data-Driven Policy

DON'T TRUST BUT VERIFY: STRENGTHENING U.S. LEADERSHIP TO SAFEGUARD OUR CYBER DEFENSES

The Case for Action

High-profile cyber breaches risk undermining confidence in the ability of the federal government and U.S. technology sector to protect and secure our critical infrastructure and government operations.

Beyond the hacks that make the headlines, there are thousands of successful cyber attacks daily on government and industry operations and critical infrastructure. The sheer scale of cyber-facilitated intellectual property theft is widely documented. China and other countries have gained decades of research for free, in what's estimated to be the largest transfer of wealth in history. Cyber technology also underpins critical infrastructure and supply chains, and cuts across many other technologies (e.g., artificial intelligence, quantum computing, financial services, microelectronics, advanced manufacturing, and virtually all innovation fronts).

Despite widespread consensus on the importance of improving cybersecurity, cyber risks continue to proliferate given an insufficient implementation of cyber defenses. This gap leaves America's critical infrastructure vulnerable to exploitation. The adversarial landscape ranges from nation-state-funded organizations to international criminal hacking groups. These threats must be met with informed and persistent leadership and determined actions by asset owners and operators.

Key Challenges and Opportunities

While some cyber risks are well-known and understood, others are emerging with little consensus on how to protect against them and what future challenges they might pose. What's clear is that critical infrastructure is at risk, the cost of cyber crime is rising, cyber threats are global in scope, emerging technologies present concerns, and zero trust and assurance are crucial. Most important, effective U.S. leadership is essential.

Critical infrastructure faces existential threats, and our cyber adversaries are clear about their intentions. Senior U.S. officials have publicly acknowledged the scale of China's efforts to exploit vulnerabilities in our infrastructure networks—electric power, dams, water systems,[1] manufacturing, and even military systems. Our financial sector is also a target and, even though it has sophisticated and mature cyber defenses, its focus is on countering fraud from organized crime—not large-scale disruptive and destructive cyber attacks from nation states. In reality, most organizations remain reactionary and lack the resources to mount an effective defense from a national adversary. Those with resources often have poor risk calculation and prioritization. Rather than proactively identifying adversary actions, organizations often operate with a focus on security regulations, procedures, and patch management, most of which are ineffective against sophisticated adversaries.

4 Recommendations for Safeguarding Cyber Defenses

Protect critical infrastructure

Implement zero trust and SBOMs

Prepare for quantum computing

Clarify and strengthen authorities

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Critical infrastructure owners and operators face a myriad of uncoordinated guidance with multiple existing standards that further complicate implementing effective security practices. Sector Risk Management Agencies do not adequately enable each sector to self-evaluate its specific risks, identify specific improvements in vulnerability and assurance, and improve cross-sector information sharing.[2] The current and complex mechanisms for coordination across the federal government and with state, local, tribal, and territorial (SLTT) governments and critical infrastructure operators don't work. Instead of viewing the federal government as a trusted partner, operators are often reluctant to engage and have expressed concern that regulations to counter cyber risks may also harm their businesses. This results in a security posture that is increasingly arduous to maintain, too often reflects a checklist rather than a risk management perspective, and consistently falls short relative to adversaries' persistence. Although the federal government has helped drive industry to create tools for generating software bills of materials, there is insufficient accountability for prevention, remediation, and mitigation of vulnerabilities.

Cyber crimes are costly. The proliferation of ransomware attacks is becoming a national crisis with high costs to industry and individuals. The Federal Bureau of Investigation (FBI) estimates that losses from cyber crime overall in the United States exceeded $12.5 billion in 2023 alone. The most frequent targets for ransomware attacks in 2023 were the healthcare and public health sector, followed by critical manufacturing and government facilities.[3] Reining in the explosive growth of ransomware attacks means directly addressing the incentive structures that have produced this crisis.[4]

Threat actors know no geographic boundaries and successful attacks against one nation can impact systems around the world, including those of our allies and closest partners. The U.S. intelligence community has assessed that persistent cyber actors such as China and Russia appear to be shifting tactics from traditional infrastructure impacts toward impacts that hit society at large with a goal of changing our political calculus and inducing societal panic. Meanwhile, terrorist organizations have lost ground in the physical space. Given the explosion of open source artificial intelligence technologies, the next evolution of terrorism[5] could involve cyber strategies and tactics. Terrorist groups already make heavy use of cyber and digital technologies for recruitment and influence. The accessibility and availability of cyber resources now allow any interested party to employ malicious cyber tools; cause significant disruption; and instill fear, panic, and chaos. Compared with criminal actors who are financially motivated, terrorist threat actors are intent on destruction, harm, and/or degradation of trust in government. A strong U.S. cybersecurity posture therefore requires significant political and economic investment at home, along with global leadership and cyber defense capacity building among willing partners around the world.

Instead of viewing the federal government as a trusted partner, operators are often reluctant to engage and have expressed concern that regulations to counter cyber risks may also harm their businesses.

Emerging technologies present new threats and an opportunity for cybersecurity leadership. The data we are encrypting securely today—from financial and personal identification information to military operations and intelligence data—could be quickly decrypted in the future by an adversary with access to *quantum computing*. Defending against this threat will require quantum-resistant algorithms to be deployed everywhere long-term security is needed. With the rapidly increasing use of outer space for commercial and military purposes, *space assets* (e.g., satellites, vehicles) will also require new techniques for their protection and defense. Meanwhile, the United States could better deploy *artificial intelligence* (AI) to our defensive advantage while it is already being weaponized for malicious ends and to facilitate malicious actors' ability to find cyber weaknesses. AI capabilities have advanced so rapidly that security considerations have struggled to keep pace and have sometimes been overlooked.

"Do not trust, but verify" is the new norm for cybersecurity. Along with the traditional laptops, phones, and servers at risk, Americans now must protect an exponentially growing number of devices—like cars, appliances, and drones—from cyber intrusions. This requires new cyber infrastructure techniques and robust identity and access management. The U.S. government and the private sector have begun implementing the *Zero Trust Model* (ZT) for technology, which assumes that no actor, system, network, or service operating outside or within the security perimeter is trusted. ZT also presumes there are, or could be, compromised components at any time. This model requires continual verification of anything and everything

attempting to establish access and allows communication among devices on a "need to know" basis. In addition, there is a growing recognition that both government and private sector systems are likely to have compromised components, which requires coupling cyber defenses with *cyber resilience*[6] (e.g., the assured ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources, including for weapons systems and defense infrastructure), *threat hunting* (e.g., a proactive approach to identifying threats that may already be present within the system, rather than waiting for an alert or incident to occur), and *adversary engagement* (e.g., deception environments and honey tokens that not only trigger detection but provide deeper insights into adversary tactics, techniques, and procedures).

Effective U.S. government leadership is essential to address the challenges above. While cyber is a shared responsibility—including by the federal government, many sectors, critical infrastructure owners and operators, and SLTT governments—our success depends on effective leadership. However, the responsibilities and authorities for cybersecurity are divided among U.S. government departments, agencies, and offices. Decision-making authority can be fragmented, overlapping, and unclear. Stakeholders on Capitol Hill also recognize the current shortcomings of coordination and collaboration, which is one of the motivations behind the draft Federal Information Security Modernization Act of 2023 legislation. In addition to organizational and regulatory harmonization, the executive branch should lead a thorough assessment of U.S. cyber health, including better support and mitigation assistance to infrastructure, standardized reporting of cyber incidents, and collaborative engagement among federal agencies, stakeholders, asset owners and operators, and SLTT governments. Increased cyber defense capacity and growth within the U.S. workforce are needed, but they will not be fully effective without also addressing the shortcomings of current operations across the U.S. government. Meeting these needs requires improvements in processes and technology as well as budgetary alignment.

Cyber Priorities for the Incoming Administration

While there is a history of Administrations developing strategies and taking positive steps forward on cyber defense, many challenges remain. MITRE recommends the next Administration build momentum on current efforts and prioritize the following:

1. **Implement measures to protect critical infrastructure.** Now is the time for an urgent focus on actions to protect our nation's critical infrastructure from the risks that are known and on the horizon. As MITRE has communicated to the White House and in Congressional testimony,[7] this includes:

- **The Department of Homeland Security updating the National Preparedness System to account for large-scale critical infrastructure attacks**. Within six months, modify and update recovery plans across sectors that can be activated during major or extended cyber attack scenarios, similar to current planning for natural disasters.[8] The first implementation of such plans should not take place during a crisis. Instead, the existing Emergency Service Function construct can be adapted to large-scale, multiple-location, multi-domain critical infrastructure attacks. Field exercises and simulations[9] should focus on hardening and resilience activities in advance of possible nation-state-level attacks as well as on clarifying roles and responsibilities within the U.S. government and with other stakeholders.
- **Requiring zero trust principles for operational technology.** This means executing the complex but necessary upgrades to legacy systems in order to fully implement ZT, including multifactor authentication access systems and micro-segmentation. This must also be coupled with cyber resilience, threat hunting, and adversary engagement.
- **Operationalizing software bill of materials (SBOM) for critical infrastructure systems** by putting vendors on legal notice to act, including by mandating vulnerability remediation by software product providers, robust tools for assessing risk, and prompt mitigation based on discovered vulnerabilities; and expanding SBOMs to list the cryptographic details of the software.
- Within 90 days **exploring new partnership models** that provide additional federal support to critical infrastructure to systematically close gaps that threaten our national security. Options include creating a national clearinghouse to evaluate software and supply chain security and assurance best practices, and establishing a federally funded research and development center for critical infrastructure that is staffed with subject matter experts, can anonymize incoming data, and is trusted by operators and SLTT governments.

2. **Implement zero trust and SBOMs.** Cyber defense of the federal government itself is essential to ensuring continuity of operations and maintaining public confidence in the face of aggressive attacks by adversaries. The U.S. government needs to continue to capitalize on modern technology while also avoiding disruption by malicious cyber actors. As with critical infrastructure, accomplishing this for the federal government includes:
   - **Migrating the federal government fully to a zero trust architecture.** Within six months, there should be a thorough assessment of the government's zero trust maturity, completion of a government-wide implementation of zero trust principles and practices, and implementation of identity and access management principles consistent with modern standards for secure credentials and multifactor authentication and micro-segmentation.
   - **Operationalizing SBOMs across the U.S. government** by similarly holding vendors accountable to provide vulnerability remediation, tools for assessing risk, and prompt mitigation, and by including cryptographic details in SBOMs.
3. **Prepare for quantum computing to surpass current cryptographic systems.** While it is hard to predict precisely when quantum computing will crack the current encryption, the U.S. government must prepare now to protect data—past, present, and future—in the context of post-quantum cryptography (PQC). This includes:
   - Within six months, assessing the government's PQC readiness based on National Institute of Standards and Technology (NIST) standards.
   - Using cryptographic bill of materials information to create a roadmap of what systems need transitioning to PQC.
   - Leveraging the expertise of the PQC Coalition that MITRE founded to facilitate global adoption of PQC in commercial and open-source technologies.[10]
4. **Clarify and strengthen roles and responsibilities of key cyber leaders and organizations.** The United States cannot address the first three priorities without more cohesive and coordinated leadership at the federal level. Currently, cybersecurity authorities, roles, and responsibilities are shared across the U.S. government, including the National Cybersecurity Director, Federal Chief Information Security Officer, Deputy National Security Advisor for Cyber, Cybersecurity and Infrastructure Security Agency (CISA) Director, NIST, U.S. Cyber Command, FBI, and intelligence community. Within the first 90 days, the incoming administration should:
   - Complete a comprehensive mapping and clarification of the cybersecurity authorities, roles, and responsibilities across the key U.S. government leadership offices.
   - Expand the authorities at select agencies to improve execution and explore the merits of turning CISA into an independent agency.

MITRE Resources and Support

MITRE brings over 50 years of experience in cybersecurity, directly addressing advanced persistent threats and working across national security, civil sectors, and industry.[11] Our multidisciplinary cybersecurity expertise has advanced secure architectures and defensive cyber operations, developed innovative cybersecurity solutions, and analyzed the cybersecurity implications of new and emerging technologies and applications. We have a long history of safeguarding critical infrastructure and government operations in collaboration with various U.S. government departments, agencies, and offices. MITRE has been recognized for its game-changing innovations, such as CVE® (which identifies, catalogs, and defines vulnerabilities) and ATT&CK® (a globally accessible database of adversary behaviors). MITRE's whole-of-nation approach also includes efforts to strengthen the cyber capacity of allies and partner nations.

- ***MITRE Cybersecurity Fact Sheet.*** Summarizes the innovative resources and capabilities MITRE has developed and that are widely adopted and used today.
- ***2024 Testimony before the House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection.*** Provides detailed insights into the current threat environment and the need for a strategic posture, with a specific focus on the water sector.
- ***MITRE's Response to the ONCD RFI on Cybersecurity Regulatory Harmonization.*** Conveys MITRE's input to the Office of the National Cyber Director (ONCD) and recommends cybersecurity regulations focus on strengthening risk management mechanisms, tailoring support to individual critical infrastructure sectors, and enhancing the organizational capacity and expertise of Sector Risk Management Agencies.

- ***Stronger Together: Critical Infrastructure Resilience Through a Shared Operational Environment.*** Underscores the importance of robust public-private partnerships and a shared operational environment in defending U.S. critical infrastructure from adversaries' cyber operations.

About the Center for Data-Driven Policy

The Center for Data-Driven Policy, bolstered by the extensive expertise of MITRE's approximately 10,000 employees, provides impartial, evidence-based, and nonpartisan insights to inform government policy decisions. MITRE, which operates several federally funded research and development centers, is prohibited from lobbying. Furthermore, we do not develop products, have no owners or shareholders, and do not compete with industry. This unique position, combined with MITRE's unwavering commitment to scientific integrity and to work in the public interest, empowers the Center to conduct thorough policy analyses free from political or commercial pressures that could influence our decision-making process, technical findings, or policy recommendations. This ensures our approach and recommendations remain genuinely objective and data-driven.

Connect with us at policy@mitre.org

Endnotes

[1] https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party

[2] This includes Infrastructure Susceptibility Analysis, a methodology that helps prioritize risks. https://www.mitre.org/news-insights/fact-sheet/infrastructure-susceptibility-analysis-and-assessments

[3] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[4] https://www.mitre.org/news-insights/publication/breaking-ransomware-cycle-us-national-policy-options

[5] https://www.mitre.org/sites/default/files/2023-08/PR-23-2636-IAN20-Using-Intent-Based-Indications-and-Warning-to-Prevent-Terrorist-Cyber-Attacks.pdf

[6] https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

[7] https://homeland.house.gov/wp-content/uploads/2024/02/2024-02-06-CIP-HRG-Testimony.pdf

[8] https://www.mitre.org/sites/default/files/2023-11/PR-23-02057-08-Cybersecurity-Regulatory-Harmonization.pdf

[9] https://www.mitre.org/news-insights/impact-story/mitre-simextm-live-action-simulations-test-ideas-save-money

[10] https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-launches

[11] https://www.mitre.org/focus-areas/cybersecurity