BLUEPRINT FOR A NATIONAL CYBER SECURITY STRATEGY

November 2025

PRESENTED BY:

Michael T. Flynn

LTG, U.S. Army (Retired)

with Jeff Hoffmann, Senior Cyber Fellow
Gold Institute for International Strategy

ADVISORY NOTICE & COPYRIGHT STATEMENT

LETTER FROM THE CHAIRMAN

My fellow Americans, the United States is under a national emergency to deter, mitigate, and defeat foreign and domestic adversary cyber.[1] For over 35 years, the threat and impact of cyber compromises have plagued our country's national security, economy, and citizens. This existential threat that America faces is due to inaction to secure our cyber borders, which is none less than a form of invasion. The multiple cyberspace war fronts are corroding our ability to protect our national critical infrastructure. Adversary cyber activities are also decreasing the ability for state and local governments and municipal organizations to afford and provide basic cybersecurity services, which will further erode trust in our federal government.

From a historical context, the Morris Worm in 1988 has been affiliated with one of the first cyber-attacks that impacted many American universities and federal research centers to include Johns Hopkins, the National Aeronautics and Space Administration (NASA), and the Lawrence Livermore National Laboratory. The activity affected over 6,000 of the estimated 60,000 computers that were connected to the national electronic network (had the internet existed at this time). This activity involved a domestic U.S. insider with a guilty plea that led to one of the first uses of the 1986 Computer Fraud and Abuse Act.

In the late 90's, foreign State-sponsor cyber capabilities began to emerge, witnessed by the People's Republic of China (PRC) Titan Rain and the Russian Moonlight Maze campaigns, both targeting and penetrating U.S. government (USG) and military networks, designed to steal U.S. Defense Industry intellectual property (IP) and gain a greater understanding of national U.S. critical infrastructure (USCI).

By September 30, 2001, the second Quadrennial Defense Review (QDR) had emphasized the emergence of new arenas of military competition in space and cyberspace quoting, "states will likely develop offensive information operations and be compelled to devote resources to protecting critical information infrastructure from disruption, either physically or through cyberspace."[2]

Since 2001, foreign cyber capabilities have continued to advance, including expanded adversaries like North Korea's use of disruptive network wiper malware against Sony Pictures. Alongside, America's first National Strategy to Secure Cyberspace was published in 2003 with multiple Presidential Policy Directives (PPD) and the National Infrastructure Protection Plan (NIPP 2013). This new guidance integrated physical and cyber security planning and provided a framework for the federal government to coordinate with USCI owners and operators to improve information sharing and collaboratively develop risk-based approaches to cybersecurity.

While the Director of the Defense Intelligence Agency (DIA) from 2012-2014, our efforts established the "ground roots" of cyber threat intelligence (CTI) integration guided by my VISION 2020 strategy. This strategy planned for intelligence information (including CTI) to drive operations and serve as a change in the intelligence environment to be used by future administrations.

Following my tenure at DIA, cyber-attacks continued to escalate with greater scale and impact like WannaCry and NotPetya that crippled the UK's National Health Service and Ukraine's electric grid, respectively. This prompted Executive Order 13800, which solidified a foundation for *Cybersecurity of America*, leading to a renewed National Cyber Strategy in 2018 that established the following goals:

- Defend the homeland by protecting networks, systems, functions, and data;
- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;

- ❖ Preserve peace and security by strengthening the ability of the U.S. — in concert with allies and partners — to deter and, if necessary, punish adversary cyber for their "red line" activities; and,
- ❖ Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

Despite the successes in U.S. cyber strategy and policy through 2018, a drastic turn began to transform our federal government and eventually diminished trust in the constitutional framework that is supposed to be managed by an oath and a duty to protect the United States of America.

Instead, and as highlighted in my 2025 Gold Institute National Security Strategy (NSS)[3], "the U.S. now confronts a threat of unprecedented character, scope, and immediacy – and what was once NSS for geopolitical confrontation abroad, is now a fight against an enemy within our own borders." This includes dangerous undercurrents in Congress and Executive Agencies like the CIA that engaged in planning for an overthrow of our American government. This radical Left campaign led to other initiatives, such as the authorization of the Federal Bureau of Investigation (FBI) to spy on U.S. Senators, parents who opposed gender identity programs in their schools, and U.S. citizens who participated in specific religious organizations.

Meanwhile, in cyberspace from 2020 to 2024, the Office of Director of National Intelligence (ODNI) assessed that over 30 countries had obtained cyber-attack capabilities and non-State sponsored ransomware actors were transforming into cartel networks.[4] America also witnessed two major cyber-attacks that infiltrated supply chain software and led to fuel shortages in our pipelines.

Today, China (or the PRC) is pre-positioned in multiple USCI networks on U.S. soil and continues to challenge the vulnerable, uncontested U.S. cyberspace boundaries.[5] Further, Iran has proven a desire to use cyber in a hybrid warfare environment by trying to sabotage water treatment facilities in Israel, which reveals its flexible political will to use cyber for destruction and enable proxy terror actors like Cyber Hezbollah.

The expanded threat space across the digital domain, combined with advanced adversary cyber and erosion of Institutional trust in our federal government demands an America esprit de corps to fundamentally re-shape the focus on education, economy, and security versus political activism.

This includes protection of our digital domain that requires defining the American Information Environment (AIE), fully understanding the damage and new threats and renewing focus on solutions, which our Gold Institute **Blueprint for a National Cyber Security Strategy** presents.

As America approaches 250 years of sovereign existence, we owe a renewed trust and increased safety and security to our citizens and our country, all now living in a vastly more volatile information age. The American Information Environment is now, more than ever, exposed and vulnerable to adversary cyber threats, and far more dependent on interconnectivity. These factors, along with the emergence of Artificial Intelligence, greatly increases the vulnerability of our nation over the next quarter century. It's time we better prepare for the future.

Honorable Michael T. Flynn
Lieutenant General, U.S. Army (Retired)
25th National Security Advisor to the President of the United States
Chairman, The Gold Institute for International Strategy

Table of Contents

Introduction and Executive Summary ---- 6

Foundations for Cybersecurity and Digital Transformation ---- 6

- *Framework for Shaping a National Cyber Security Strategy* ---- 7

White House Executive Requirements 9

Cybersecurity Laws in the United States 11

Pillar I. Assess the Damage of Compromise ---- 11

Pillar II. Address the National Emergency to Deter, Mitigate, and Defeat Foreign Adversary Cyber 13

Organization 14

Operations and Response 14

- *Authorities for Offensive and Defensive Cyber Operations* ---- 16
- *Expanded Adversary Cyber Threat with Risk for Greater Consequences* ---- 16

Pillar III. Respond to Shortfalls in Cybersecurity to Strengthen National Security at Home and Abroad ---- 19

Pillar IV. Rebuild Partnerships and Processes for Improved Cyber Threat Information Sharing ---- 20

Pillar V. Defend and Leverage Emerging Technologies and Innovation to Advance Capabilities in Cyberspace ---- 22

- *The Next Big Cyber Threat from Quantum Computers…Is the Government Ready?* ---- *22*
- *The Risks of Uncertainty* ---- 23
- *Leverage Knowledge of Cyber Threats to Expedite Zero Day Solutions Across the AIE* ---- 24

Conclusion ---- 25

Glossary of Acronyms ---- 27

Bibliography ---- 29

Introduction and Executive Summary

The purpose of this **Blueprint for a National Cyber Security Strategy** is to provide a framework of ideas to assist both the public sector, including policymakers and private sector leaders with the development of strategic concepts for cybersecurity solutions. This Blueprint provides a resource of information and ten recommendations that, if enacted, can reorganize structure and leadership and build strategy, policy, operations, risk management plans, partnerships, and workforce development for cyber and digital transformation for the 21st Century.

The Blueprint is founded on fact-based research like the initial fiscal year (FY) 2019 Cyberspace Solarium Commission and over four Government Accountability Office (GAO) high-risk priority shortfall reports. Since January 2023, these GAO reports have called for urgent action to address cybersecurity challenges, including the implementation of White House Executive Order (EO) requirements.[6]

Combining cybersecurity gaps with the 2025 White House Artificial Intelligence (AI) Action Plan[7] policy actions is one finding in this Blueprint that provides baseline frameworks for incident response, threat intelligence information sharing, skill-set development, research, and international cooperation.

Despite noble but aspirational strategic objectives since 2023, our adversaries in cyberspace continue to successfully target and grow capabilities to compromise technologies in the digital domain that are the backbone of our nation's security. These activities weigh a financial burden on organizations that, according to a 2024 IBM report, cost the U.S. over $10.2 million (average per incident).[8] To put this into perspective, there were over 3,158 known cyber breaches reported[9] in 2024 for total cost of over $32 billion to address post-compromise incidents with little to show in accountability or response to adversary cyber.

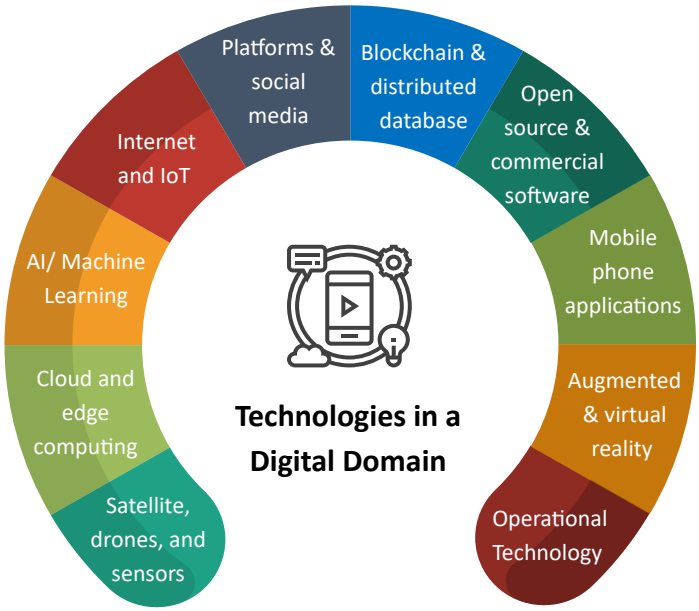
The costs of these breaches demand immediate mitigation plans and strategy, de-emphasizing other 2023 National Cyber Strategy Implementation objectives like Secure Our Clean Energy Future and workforce development plans that benefit from prioritized and politically charged diversity, equity, and inclusion (DEI) programs and incentives.[10]

Cybersecurity for the 21st Century must focus on practical, measurable objectives that strengthen the security of the digital domain that benefits the American people and economy every day. Objectives should include emphasis on development of expanded "left of boom" offensive capabilities with better intelligence that drives operations, deterrence policy that aims to defeat our cyber adversaries, along with design of more affordable risk management plans and practices. This includes the evaluation of cyber compromise damage to USCI and networks.

Foundations for Cybersecurity and Digital Transformation

Today's AIE poses new and complex challenges for national security. The shift to the information age, advances in information technology (IT), wireless communications, and social media have increased the speed and range of information, diffused power over information, and transformed socio-cultural norms.

The graphic below summarizes an overview of the evolving AIE that a **National Cyber Security Strategy** can update and better define.[i11]



The AIE is not only a physical place, nor is it a purely a virtual platform with several cloud computing services like software, platform, and infrastructure. In the AIE, computers and cloud environments store data combined with systems and infrastructures that allow data and information to flow. Examples: Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, operational technologies (OT), and space-based communications.

The 2025 AI Action Plan affirms that high-quality data has become a national strategic asset as governments pursue AI innovation goals and capitalize on technology's economic benefits. Quoting, "other countries, including our adversaries, have raced ahead of us in amassing vast troves of scientific data. The U.S. must lead the creation of the world's largest and highest quality AI-ready scientific datasets, while maintaining respect for individual rights and ensuring civil liberties, privacy, and confidentiality protections."

America and its allies must also defend against the corruption of massive global data sets that may have been polluted through disinformation campaigns by malign nations and domestic actors. This includes our own U.S. mainstream media use of AI large language model tools to skew results towards a bias public opinion (as one example).

Framework for Shaping a National Cyber Security Strategy

To accomplish goals for cyber and digital transformation in the 21st Century, a new bipartisan, integrated interagency approach must be enacted that leverages initial "selected" recommendations from the CSC and addresses GAO reporting shortfalls. Two common ground recommendations include reforming the government's structure and organization for cyberspace and addressing GAO recommendations. Other strategic concepts can be considered from the McCrary Institute 2025 Presidential Transition Task Force

[i] The Department of War defines the IE as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information- consisting of physical, informational, and cognitive dimensions.

(PTTF) report[12], and renewed guidance and direction from a series of Presidential Policy Directives (PPDs), EOs, and legislation.

The CSC was established in the National Defense Authorization Act for FY 2019 to "develop a consensus on a strategic approach to defending the U.S. in cyberspace against cyber-attacks of significant consequences."[ii]

CSC recommendations were organized into six pillars:

1. Reform the U.S. Government's Structure and Organization for Cyberspace.
2. Strengthen Norms and Non-Military Tools.
3. Promote National Resilience.
4. Reshape the Cyber Ecosystem.
5. Operationalize Cybersecurity Collaboration with the Private Sector.
6. Preserve and Employ the Military Instrument of National Power.

In comparison, the 2023 U.S. National Cybersecurity Strategy established five pillars:

1. Defend USCI.
2. Disrupt and Dismantle Threat Actors.
3. Shape Market Forces to Drive Security and Resilience.
4. Invest in a Resilient Future.
5. Forge International Partnership to Pursue Shared Goals.

Alongside the National Strategy, in August 2023, America's primary cyber defense agency, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) published a Strategic Plan for FY24-FY26. This plan focused on three goals: Address the immediate threat, drive security at scale, and harden the terrain.[13]

The 2023 Strategy and follow-on Implementation Plans[14] guided some important initiatives like the update of the National Cyber Incident Response Plan (NCIRP), directed the Department of War (DoW) to develop a cyber strategy[15], and established funding incentives through the Bipartisan Infrastructure Law for improved USCI cybersecurity. In September 2022, to complement investment initiatives, CISA established the State and Local Cybersecurity Grant Program (SLGCP), which recently received $103.8 million for a range of cybersecurity improvements to assist state, local, tribal, and territorial (SLTT) organizations. Assistance has included planning and exercises, hiring cyber experts in the community, and improved delivery of managed shared services like vulnerability management assessments for USCI organizations.

[ii] www.solarium.gov. The CSC drew its inspiration from President Dwight D. Eisenhower's 1953 Project Solarium. Eisenhower tasked his national security team with designing a long-term competitive strategy that would outlast his presidency. Project Solarium consisted of three teams, each developing a different strategic framework, against each other over the course of six weeks at the National War College with a day-long debate at the White House. This work eventually became NSC 162/2 – Eisenhower's "New Look" grand strategy for successful containment policy against the Soviet Union.

White House Executive Requirements

❖ *EO for Ending the Weaponization of the Federal Government, January 20, 2025*

While not directly related to cyber and digital transformation, this EO highlights the Department of Justice (DOJ) punishment of an individual for posting a political meme with impacts that could affect several federal government agencies directed by PPD or designated with lead roles to implement national cyber strategy and implementation plan objectives.

❖ *EO for Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending EO 13694 and EO 14144, June 6, 2025*

Affirmed that the PRC continues to present the most active and persistent cyber threat to USG, private sector, and USCI networks. This has been apparent in the recent use of a series of Chinese Typhoon Advanced Persistent Threats (APTs) aimed at American CI organizations like telecommunications, transportation (i.e. maritime), manufacturing, and education.[16] Chinese cyber activities were also affiliated with 2020 election interference activities by accessing voter registration data.[17]

While the EO highlights continued threats from Russia, Iran, and North Korea, a new 21st Strategic Cyber Approach must assess and consider threats from other actors, both domestic and abroad. These could include newly designated terror groups like Antifa, cartel technology advances and use of cyber against American border control infrastructure. Additional adversaries will continue to grow, such as radical Islamic roots who are opposed to Western principles and doctrine and more advanced cyber criminals.

This EO provides directions to the Secretary of Commerce and Director of the National Institute of Standards (NIST) to establish a consortium with industry at the National Cybersecurity Center of Excellence for secure software development and to update NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations. The Presidential Order also provides new guidance related to quantum computing, U.S. Cyber Trust Mark for Internet-of-Things (IoT), and security for AI.

Quoted by President Donald J. Trump in the 2025 AI Action Plan:

> "Today, a new frontier of scientific discovery lies before us, defined by transformative technologies such as AI… Breakthroughs in these fields have the potential to reshape the global balance of power, spark entirely new industries, and revolutionize the way we live and work. As our global competitors race to exploit these technologies, it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance. To secure our future, we must harness the full power of American innovation."

The EO states that, "AI has the potential to transform cyber defense by identifying vulnerabilities, increasing the scale of threat detection techniques, and automating several components of a CTI program to include information sharing platforms."

❖ *EO 14028, Improving the Nation's Cybersecurity," May 12, 2021*

Provided guidance that aimed to remove barriers to sharing CTI, focused on initiatives to modernize federal government cybersecurity like Zero Trust Architecture (ZTA) and use of FedRAMP for cloud security, and directed the Secretary of Commerce and Director of NIST to develop guidance for software supply chain security, including the use of a Software Bill of Materials. This EO also provided direction

for the review and better stand-up of practices for cyber incident response like refinement of the Cyber Unified Coordination Group (UCG). The EO also called for the standardization of a set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability assessment and incident response activity against Federal Civilian Executive Branch (FCEB) information systems.

❖ *EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017*

Following this EO, the 2018 National Cyber Strategy[18] was published that hadn't been produced for 15 years. Four strategy objectives included:

- Defend the homeland by protecting networks, systems, functions, and data;
- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
- Preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and
- Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

The EO enforced risk management plans and procedures, including use of *The Framework for Improving Critical Infrastructure Security*. The establishment of CISA can be attributed to this EO and directed the Secretary of Energy to assess cyber incident response capabilities in the case of a disruption to American's electrical grid.

EO 13800 directed the Secretary of War (Defense at the time) to lead an assessment of cybersecurity risks that faced the defense industrial base (DIB), including its supply chain, and U.S. military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks.

This EO also laid the foundation for *Cybersecurity of America* focused on three primary areas: a deterrence and protection plan against cyber adversaries, international cooperation, and workforce development.

❖ *PPD 41, "United States Cyber Incident Coordination," July 26, 2016*

Established three lines of effort to respond to any cyber incident involving government or private-sector entities: (1) threat response; (2) asset response; and (3) intelligence support and related activities. This PPD provided guidance for National Policy Coordination through the Cyber Response Group and led to the establishment of the Cyber UCG, later codified into NCIRP and NIST Interagency Report, "Prioritizing Cybersecurity Risk for Enterprise Risk Management." This PPD also led to the development and use of Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government.

❖ *PPD 21, "Critical Infrastructure Security and Resilience," February 12, 2013*

Published on same day as EO 13636, "Improving Critical Infrastructure Cybersecurity," that built on PPD 63, "Critical Infrastructure Protection: Sector Coordinators," published August 5, 1998. Combined EO/PPDs led to the identification and refinement of USCI functions, roles, and responsibilities across the federal government with guidance for improved coordination and collaboration through the Sector-Specific Agencies or what are presently known as the Sector Risk Management Agencies (SRMAs). EO 13636 also led to NIPP 2013, "Partnering for CI Security and Resilience." This National Plan integrated

physical and cyber security planning and provided a framework for the federal government to coordinate with USCI owners and operators to improve information sharing and collaboratively develop and implement risk-based approaches to cybersecurity. The National Plan categorized risks aligned with PPD 8 across the five national preparedness mission areas of prevention, protection, mitigation, response, and recovery.

Cybersecurity Laws in the United States

Cybersecurity laws in the U.S. continue to evolve in response to the increasing reliance on technologies in the AIE and the growing threats posed by cyber adversaries. These laws aim to protect individuals, businesses, and government agencies from unauthorized access, data breaches, and other cybercrimes. The regulatory landscape is shaped by federal statutes, state laws, and industry-specific regulations, each addressing different aspects of cybersecurity and data protection. Notable federal laws include:

- **Cybersecurity Information Sharing Act (CISA) of 2015 (soon to expire without renewal).** CISA encouraged private sector companies and government agencies to share information about cybersecurity threats and incidents. The goal was to enhance collective defense and response capabilities while protecting privacy and civil liberties.

- **Federal Information Security Modernization Act (FISMA) of 2014.** FISMA sets out requirements for federal agencies to develop, document, and implement programs to secure their information systems. It also establishes a framework for continuous monitoring and reporting of cybersecurity practices.

- **National Cybersecurity Protection Act of 2014.** Established the National Cybersecurity and Communications Integration Center within the DHS.

- **Cybersecurity Enhancement Act of 2014.** Supports research, development, and public-private partnerships to improve cybersecurity practices across sectors.

- **Computer Fraud and Abuse Act (CFAA) of 1986.** The CFAA is one of the foundational statutes addressing computer-related offenses in the U.S. It criminalizes unauthorized access to computer systems, data theft, and other forms of computer fraud. The law has been amended multiple times to keep pace with technological changes and emerging threats.

Through EOs, PPDs, and legislation, the USG sets the strategic direction, operational requirements, and legal frameworks for cybersecurity. This strategy identifies five pillars with recommended actions that collectively aim to strengthen action against cyber threats, facilitate collaboration between public and private sectors, and protect USCI and information systems.

Pillar I. Assess the Damage of Compromise

As digital transformation accelerates, organizations and individuals are increasingly dependent on cyberspace for essential operations, communication, and data management. This reliance exposes them to a variety of threats and impacts that become a critical concern, including financial costs, operational disruption, legal and regulatory consequences, and loss of IP. Prioritized assessment should include entities that are a dependency and retain trade secrets for the U.S. DIB, like an academic institute or DIB companies working on national security assets ranging from weapons systems to hardware.

Assessing the damage following a cyber compromise is essential for effective response, recovery, and future risk mitigation. Cyber compromise can occur in various forms, including:

- Data Breaches (for cybercrime or espionage): Unauthorized access to sensitive data such as personal information, financial records, national security information or IP.
- Ransomware Attacks: Malware encrypts files and demands payment for decryption.
- Denial-of-Service (DoS) Attacks: Systems are overwhelmed, making services unavailable to legitimate users.
- Phishing and Social Engineering: Manipulation of users to gain access to confidential information.
- Insider Threats: Employees or trusted individuals misuse their access for malicious purposes.
- Supply Chain Attacks: Compromising third-party vendors to reach the ultimate target.
- Advanced Persistent Threats (APTs): Long-term, stealthy presence in networks, often from state-sponsored or highly sophisticated criminal groups with a focus on intelligence gathering and maintaining access.

The threat of cyberattacks against USCI has evolved beyond data theft and espionage. In February 2024, CISA, the National Security Agency (NSA), and Federal Bureau of Investigation (FBI) published an advisory[19] that assessed PRC State-sponsored cyber actors that are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against USCI in the event of a major crisis or conflict with the U.S. The PRC's Volt Typhoon has compromised the IT environments of multiple CI organizations—primarily in communications, energy, transportation systems, and water and wastewater systems sectors. Volt Typhoon's choice of targets and patterns of behavior is not consistent with traditional cyber espionage or intelligence collection operations. The advisory assessed with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement in OT assets to disrupt functions.

The CSC designed a three-layer deterrence model for cyberspace aimed to reduce the frequency and severity of cyber-attacks of significant consequences. The final layer proposed recommendations related to costs to build cyber capabilities and capacity. Like any requirement building process, it is impossible to align costs to requirements or needs without a proper baseline understanding of the threat landscape, adversary compromise impact, and expense for mitigation.

RECOMMENDATION: ONCD direct that ODNI, in collaboration with CISA and selected private sector cybersecurity organizations conduct a detailed assessment of adversary cyber compromise against the U.S. Minimum components of the assessment should include:

- Overall damage assessment scope of state and non-state sponsored cyber compromise, both comprehensive and by categorized by critical infrastructure sectors;
- Specific overview of primary APT activities by country (i.e.) PRC Typhoon series;
- Forecasts of the cyber threat landscape and vulnerability assessment as part of a report that includes recommendations and costs to mitigate, deter, and defeat adversary cyber (both domestic like border control security assets and foreign). Costs should be categorized under organization, personnel, and needed capabilities (including technologies and core elements of threat intelligence and risk management plan); and
- Final report submitted to ONCD and OMB for review and action. Report should include Congressional District snapshot assessment material.

Pillar II. Address the National Emergency to Deter, Mitigate, and Defeat Foreign Adversary Cyber

On March 27, 2025, President Donald Trump renewed the national emergency to deal with the unusual and extraordinary malicious cyber-enabled threats to the U.S. national security, foreign policy, and economy. In accordance with the National Emergencies Act (50 U.S.C. 1622(d)), this order was renewed for one year and remains in effect until,

(1) There is enacted into law a joint resolution terminating the emergency; or
(2) The President issues a proclamation terminating the emergency.

Foundation for Pillar action was published in the CISA Strategic Plan FY2024-2026, which included goals that could prove to be effective in future strategy. Objectives include greater visibility of cybersecurity threats with a better understanding of how adversary cyber-attacks occur, better coordination of post-compromise forensics like disclosure of threat hunting reports, and more planning for exercises and joint cyber defense operations and incident response. CISA also produced more technical strategies focused on the development and use of advanced technologies, data integration, continuous evaluation and monitoring, and workforce development.

Despite feasible strategic goals that continue to support ongoing mitigation efforts in cybersecurity IT, there must be more emphasis and expediency on initiatives to immediately protect the entirety of the AIE. This strategy encourages the use of the "whole of nation" framework proposed in the CSC that consists of citizens, private sector, and limited government. The Framework leverages an international partner network and integrates multiple options of power as part of a three-layer deterrence strategy.

The concept of this layered strategy was founded in the 2018 DoW Cyber Strategy defined as DEFEND FORWARD.[20] DEFEND FORWARD called for the strategic competition in cyberspace that can provide baseline for a new expanded **National Cyber Security Strategy** aimed to assess and mitigate damage, fortify and deter, and deploy new operations and policy to gain advantage and dominate in the digital domain.

The **Blueprint for a National Cyber Security Strategy** consists of three primary objectives to impact organization, operations and response, and policy.

RECOMMENDATION: U.S. Senate hold session for one vote on slated list of cybersecurity leaders awaiting confirmation.

- NSC develop a list of cybersecurity leader candidates awaiting confirmation and send in Presidential Memo to the U.S. Senate, emphasizing impact to the National Emergencies Act for adversary foreign cyber (if not confirmed).
- Leadership is in dire need to affect future strategy (including possible decisions for organizational re-construct), policy, and operations.

Organization

In March 2024, the Foundation for Defense of Democracies (FDD) produced the "U.S. Cyber Force"[21] report that provided a comprehensive overview of organizational structure and issues that continue to plague cyber readiness in the U.S. military. Several of the findings directly contradict 2018 objectives to ensure that the U.S. military's ability to fight and win wars in any domain is achieved, including cyberspace.

The FDD report primarily looked at the organizational structure and personnel system of U.S. Cyber Command (CYBERCOM) since its stand-up in 2010 under U.S. Strategic Command. Still today, CYBERCOM is led by a commander who is dual hatted as the director of the NSA rather than a sovereign organization like U.S. Space Command and Force.

Common issues identified in the FDD report included low maturity level cyber operation force design, cyber workforce recruitment and retention shortfalls, lack of cyber 'cadre culture, inconsistent training and skillsets, and insufficient acquisition tools and processes for cybersecurity capabilities.

Based on one general officer's remarks in the report, "the current strategy of relying on the existing Services to build the cyber expertise and capabilities required is inefficient, ineffective, and unlikely to succeed despite years of investment and the best efforts of servicemembers." Washington's "only viable path forward," the officer said, "is to establish a new Service focused on organizing, training, and equipping forces required to fight – and win – in cyberspace."

Alongside military cyber capabilities, while the re-assessment of the civil structure of federal government through the Department of Government Efficiency was required, this unfortunately has depleted several traditional cyber resources and policies needed for this level of National Emergency. Losses include people with unique cybersecurity skillsets and expiring legislation like the CISA 2015 that diminishes the flow of vital CTI sharing. Information sharing structures have also been diminished, such as the Office of the Director of National Intelligence Cyber Threat Intelligence Integration Center (CTIIC). An entity like CTIIC could benefit from re-alignment under a new integrated, interagency framework like the UK's National Cyber Force.

Operations and Response

If resources for cybersecurity continue to be diminished while vulnerabilities in the AIE expand, challenges will only increase due to the dynamic nature of advanced cyber threats and non-standardized cyber incident response plans (CIRPs). This includes the need to integrate new guidance into existing CIRPs like NIST standards for prioritizing cybersecurity risk.

Cyber operations and response in the U.S. will continue to evolve as both government and private sector organizations, especially USCI, work to strengthen defenses against adversary cyber actors.

According to the FDD U.S. Cyber Force report and CYBERCOM reporting[22], there are over 130 Cyber Mission Force (CMF) teams, made up of both military and civilian personnel as part of the Cyberspace Operations Forces (COF). Within the COF, the CMF directs, coordinates, and executes cyber operations. CMF teams include:

- *Cyber National Mission Force (CNMF)* teams are responsible for defending the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them. These operations are largely conducted as independent campaigns, not in support of combatant command missions.

- *Cyber Combat Mission Teams* conduct military cyber operations in support of combatant commands.

- *Cyber Protection Teams* are responsible for defending the DoW information networks, protecting priority missions, and preparing cyber forces for combat.

- *Cyber Support Teams* provide analytic and planning support to CNMF and the Cyber Combat Mission Teams.

By 2026, new teams are expected to be responsible for supporting combatant commanders in space operations and countering cyber influence or adversary disinformation campaigns.

Despite what appears to be a robust capability to counter adversary cyber, America is still untested for a Level 3 (HIGH) or Level 4 (SEVERE) cyber-attack, including exercises that evaluate the threshold of failed incident response. These levels are defined as, "likely to result in demonstratable or significant impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence."

RECOMMENDATION: ONCD provide oversight, in collaboration with CYBERCOM, CISA, and ODNI to conduct an expanded Cyber Storm X.

Discoveries of USG political weaponization could suggest that past cyber activities are questionable and were not conducted in the best interests of the U.S. An effective **National Cyber Security Strategy** must be immune to external influence. This influence could have included exercise participants opposed to "Blessings of Liberty" values defined in the 2025 Gold Institute NSS.

- A new exercise should be conducted with a longer timeframe and expanded focus on "the whole of society" approach to understand American (especially USCI) organizational roles and capabilities in a cyber-attack. This exercise should incorporate changes directed under 2025 Presidential order, using real cyber actor tactics and techniques, focused on Level 3-5 (EMERGENCY) cyber-attack or "imminent threat to wide-scale CI services, national government stability, or lives of U.S. persons." Incident scenarios should include compromise and incident response of OT in a USCI sector. The exercise should have cascading impacts if the wrong actions are taken and use adversary cyber scenarios that "imagine the unimaginable."
- The goals of this exercise will be to re-assess effectiveness of national cyber organizational capabilities, plans, and incident response (which just concluded public comment); identify roles and responsibilities during a cyber incident; and examine information sharing and coordination mechanisms, including use of public-private partnerships (domestic and foreign).
- The exercise directly supports a 2024 Defense Science Board (DSB) Study recommendation on "DoD Dependencies on USCI," to normalize engagement between specific installation commanders and civilian infrastructure owners through use of tabletop exercises (TTXs) to identify uncertainties and vulnerabilities and assess risk.

Policy

One of the first foundational policies in cybersecurity was established under PPD 63 in May 1998. This PPD established a National Goal to achieve a nation-wide operating capability by the year 2000. No later than five years after the PPD signature, in 2003, the U.S. was to have achieved and maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The USG to perform essential national security missions and to ensure public health and safety.
- State and local governments to maintain order and deliver minimum essential public services.
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Authorities for Offensive and Defensive Cyber Operations

By 2010, CYBERCOM was stood up and National Security Presidential Memorandum-13 (NSPM-13), *United States Cyber Operations Policy* refined the initial principles and processes for offensive and defensive cyber operations authorized by the USG. The NSPM-13 provided greater authorities for the DoW. In 2018, CYBERCOM was elevated to a combatant command with the following rules of engagement:

- Engage the cyber adversary in the context of a named military operation; and,
- Respond to offensive adversary cyber operations directed against the U.S. and its interests.[23]

Expanded Adversary Cyber Threat with Risk for Greater Consequences

In comparison to policies, authorized operations, and military and civilian (i.e.) CISA organizations established for American cybersecurity, the 2018 ODNI Annual Threat Assessment reported that over 30 countries (as of 2017) had obtained cyber-attack capabilities. These capabilities were defined as being used for a 'low-cost tool of statecraft, which ODNI assessed that the State-sponsored cyber operations would be used to achieve strategic objectives unless they faced clear repercussions. Non-State cyber adversaries would continue to use operations for financial crime and to enable propaganda and messaging.

In February 2024, CISA, partnered with other interagency and foreign partner services published guidance to define new adversary tradecraft terminology known as "living off the land (LOTL)."[24] LOTL essentially is the pre-positioning of malware for later use, which was witnessed by the PRC's Volt Typhoon use against USCI organizations.[25] To date, there does not seem to be policy to address the escalation of advanced adversary cyber. When reviewing new response options, **National Cyber Security Strategy** needs to consider how is the deployment of cyber weapons in USCI different than China deploying ground-based air defense units in Thailand off the South China Sea like what occurred in the Falcon Strike 2025 joint training exercise.[26]

Cyber capabilities can impose significant impact as seen in Iran and Israel. According to Israel National News, "Iran experienced more than 20,000 cyber-attacks during the recent 12-day conflict with disruptions to payment systems, fuel distribution, healthcare networks, and critical infrastructure."[27] In contrast, the UK's Sky News claimed to obtain classified documents, allegedly from Iran's Shahid Kaveh, which is part of Iran's elite Islamic Revolutionary Guard Corps, that revealed secret research into how a cyber-attack could be used against CI assets like sinking a cargo ship or blowing up a fuel pump at a petrol station.[28]

RECOMMENDATION: ONCD, in collaboration with the Department of State (DOS) develop five "red line" policy memos to be shared at the Presidential level with China, Russia, Iran, and North Korea with a fifth memo to be used for all other adversaries, including cyber criminals and terrorists.

- The Memos would model Mutually Assured Destruction (MAD) deterrence policy and doctrine that highlights levels of adversary cyber activity and consequences, especially against USCI. Consequences could range from economic through use of sanctions to kinetic options for more severe Level 3-5 activities.
- Memos should incorporate consequences for pre-positioned malware. EXAMPLE: Authorization of U.S. "hack back" operations if adversary cyber activity is attributed to LOTL tradecraft or NATO Article 5 attribution and action of cyber compromise.

RECOMMENDATION: ONCD, in collaboration with DoW, DHS, and ODNI produce a Quadrennial National Cybersecurity Review (QNCR) roll-up report to assess organization, policy, and operations.

- This effort would re-establish the DoW QDR, combined with completion of a Quadrennial Homeland Security Review and Quadrennial Intelligence Community Review.
- For DoW, emphasis should be focused on re-assessment of past DSB studies like cyber warfighter capabilities and incorporation of other efforts or recommendations (i.e.) independent evaluation for creation of U.S. Cyber Force (i.e.) detachment as a Combatant Command) and separation from NSA.
- Assess needs to repurpose or develop new organizational constructs like the establishment of a National Cyber and Critical Infrastructure Security Agency (NCCISA). Modeled after the UK's National Cyber Agency through the National Cyber Security Centre and Ministry of Defense Cyber & Specialist Operations Command. Some goal objectives could include: Consolidation of Agency level cyber resources (i.e. CIA and NSA), re-alignment and strengthening of CISA Divisions like vulnerability management, shared cybersecurity services, re-establishment of a combined cyber, CI, and AI threat intelligence fusion center, review of military v. civilian Title authorities & responsibilities including State Title 32 level resources, and review of public-private partnership programs and plans like the Sector Risk Management Agency (SRMA) framework.
- Both, the National Exercise, other sector based TTXs like maritime, and QNCR could inform strategy, policies, and plans and better enable other intelligence efforts like development of requirements for technical collection, cyber counterintelligence, and increased human intelligence operations. One example of an intelligence tool is a Collection Support Brief that defines adversary cyber-APT lifecycles and components to include order-of-battle and technology supply chains.

As a secondary recommendation integrated with the QNCR, a follow-on DSB should be initiated to assess and evaluate offensive cyber options, including enhanced USG and tier authorities for private sector companies for counterattack against adversary cyber-CI, including military assets and for use in a hybrid conflict.

Cyber Workforce Shortfalls Jeopardize AIE Protection

In a September 2025 GAO report, as of April 2024, federal agencies reported an estimated 67,000 employees coded as "cyber workforce" at an annual cost of over $14 billion. Despite these numbers, GAO revealed that the data was incomplete and unreliable and reported that since 2019 of the 64 recommendations published to address cyber workforce issues; 32 of these were not yet fully implemented.[29]

Comparatively, according to a 2024 Cybersecurity Workforce report, the U.S. boasted over 2 million cybersecurity professionals with a shortage of at least 560,000, primarily in the financial services and industrial sectors. In its "State of the Tech Workforce" report[30], CompTIA highlighted that career fields in tech are expected to grow at about twice the rate of overall employment in the U.S. economy over the next 10 years.

From a policy perspective, in early 2023, ONCD established the National Cyber Workforce Coordination Group (NCWCG) and the Federal Cyber Workforce Working Group. These groups were co-chaired with OMB in consultation with Office of Personnel Management (OPM), to help advance the work that needs to be completed to implement the archived National Cyber Workforce and Education Strategy (NCWES). In November 2023, two more groups were established under the NCWCG: the Working Group on Cyber Workforce and Education and the Working Group on Cyber Skills and Awareness. Before President Trump took office in January 2025, more than 35 Federal departments and agencies in these groups had begun implementing the objectives in the NCWES.

RECOMMENDATION: ONCD, in collaboration with Department of Labor, NIST National Initiative for Cybersecurity Education (NICE), OPM and the Secretary of Education, host a National Cyber and Digital Transformation Workforce Summit to inform a re-assessment of the NCWES.

- The Summit will bring together leaders across the public and private sector (including academia) to assess the effectiveness and challenges in the NCWES and address key recommendations from the September 2025 GAO Study on Cyber Workforce.
    - Included and added to Cyber Workforce strategy, plans, and policy should include new incentives for faith-based organizations.
- Summit planning could be synchronized with the 2025 AI Action Plan policy actions to, "train a skilled workforce for AI infrastructure." Proposed activities in the Plan include creation of a national initiative to convene employers, industry groups, and other workforce stakeholders to develop or identify national skill frameworks and competency models for career fields. Frameworks would provide voluntary guidance that may inform curriculum design, credential development, and alignment of workforce investments.
- Summit could inform the update of existing programs like Career, Technical, and Adult Education programs and other partnerships with education and workforce system stakeholders. The Summit could also support congressional legislation like the Proving Individuals Various Opportunities for Technical Training (PIVOTT) Act of 2024.

Pillar III. Respond to Shortfalls in Cybersecurity to Strengthen National Security at Home and Abroad

Along with shortages in the cyber workforce, in June 2024, the GAO reported that over 30,000 security incidents were submitted to DHS in FY22. Starting in January 2023, the GAO has published several high-risk series reports on the following topics:

- Establishing a more comprehensive cybersecurity strategy;[31]
- Securing federal systems (or FCEB networks) and information; and,[32]
- Protecting the cybersecurity of USCI and privacy and sensitive data.[33] [34]

Since 2010, the GAO made over 4,000 recommendations to federal agencies to address cybersecurity shortcomings. However, more than 850 of these had not been fully implemented as of February 2023. Of these recommendations, 52 were identified as priority, to include:

- Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace – beyond a checklist of recommendations actions. Roadmaps and strategic concepts for solutions;
- Full establishment and implementation of cyber risk management programs. As one example, the most recent Defense DIB Sector Specific Plan identified under the NIPP was published in 2010;
- Development of methods for determining the level and type of adoption of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* by the CI entities; and,
- Address weaknesses in federal agency information security programs, including federal versus state role in protecting the cybersecurity of USCI.

Without addressing the shortfalls, combined private sector trends in cyber will outpace the capacity of American cybersecurity – these trends include the use and rise of GenAI, which is transforming data security programs and expanding threat space due to the dependency of GenAI, cloud services, and automation for identity and access management.

According to a Gartner survey of 162 large enterprises conducted between August and October 2024, organizations use an average of 45 cybersecurity tools. With over 3,000 cybersecurity vendors, a **National Cyber Security Strategy** needs to explore the balance of procurement and use of managed shared services to maintain the right security posture. Gartner recommends the consolidation and validation of core security controls and focus on architecture that enhances portability of data along with the development and use of threat modeling and organizational technology drivers such as AI adoption to be used to assess advanced cybersecurity needs.[35]

RECOMMENDATION: The NSC develop an Executive Order titled, "Response to National Emergency for Adversary Cyber and Shortfalls in Cybersecurity to Strengthen National Security at Home and Abroad."

- The EO will enhance EO 13800, including a mandated review of past Administration strategy and implementation plans mapped to ongoing, existing challenges identified in GAO reports (at a minimum).
- Findings will be documented in a report to OPM and Congress that identifies Executive Agent (EA) organizational roles and responsibilities for outstanding GAO report challenges.
- For existing challenges, EAs will develop roadmaps to identify action plans to mitigate. The roadmaps will include strategic concepts for solutions, not just a checklist of actions published in updated strategy or implementation plans.

Pillar IV. Rebuild Partnerships and Processes for Improved Cyber Threat Information Sharing

On the evening of September 30, 2025, the CISA 2015 legislation expired with short-term extensions proposed in the U.S. House Continuing Resolution (as of October 30, 2025). This Act includes the following provisions:

- Agencies with CTI shall have procedures to share that information in a classified and unclassified way with both federal and nonfederal entities;
- An entity (governmental or nongovernmental) can have a private sector resource monitor and secure their IT;
- Private entities may share information related to identifying and defending cyberthreats with other private entities and with the federal government;
- The private sector will not be subject to antitrust liability for participating in the cybersecurity information sharing activities authorized by the Act;
- Personally identifiable information (PII) must be removed from shared information. Further, the DHS and DOJ were mandated to develop guidance on protecting civil liberties when sharing information with additional guidance on federal government and nonfederal entity information sharing; and,
- Private entities shall be protected from liability when conducting certain Act-authorized activities, including monitoring IT, implementing protective actions, and sharing cybersecurity information.

An April 2025 Congressional Research Service (CRS) report warned that information protection measures, antitrust, liability, and protections from disclosure (i.e., in court proceedings) implemented by the Act would be impacted. Without these protections, private sector entities like CI organizations may be less willing to share CTI with the federal government.[36]

A delay or stop of the CTI exchange between the private sector and federal government will deteriorate the ability to fully understand adversary cyber actor activities. Despite the concerns, the absence of the Act's authorizations may not affect the technical capabilities DHS created to enable the Automated Information Sharing (AIS) program, which DHS was working on under different information sharing

authorities prior to the Act. Further, in March 2022, the Cyber Incident Reporting for CI Act of 2022 (CIRCIA 2022) was passed, offering alternative reporting guidance with periodic briefings provided through CISA, especially incidents involving ransomware that require an organization to make a payment.

Opportunities to Grow Cyber Threat Information Sharing

One of key policy actions in the 2025 Trump AI Action Plan is to establish an AI Information Sharing and Analysis Center (AI-ISAC) that will promote the sharing of AI-security threat information and intelligence across USCI sectors. In addition to CTI, policy actions proposed DHS develop information sharing guidance for AI that is like the CISA 2015 Act. This guidance could renew CISA 2015 that could incorporate previous unpassed Cyber Intelligence Sharing and Protection Act legislation to enable information exchange between the private sector and federal government of combined AI-CTI specific vulnerabilities and threats.

To make an ISAC more effective, the USG should also be willing to accept more risk by declassifying intelligence for the private sector, including USCI to act and incorporate into their risk management plans and information requirements. The current posture is too slanted toward preserving inactionable "secrets" and the USG risks losing relevance without their willingness to improve information sharing practices.

America First Cyber Does Not Mean America Cybersecurity Alone

The Gold Institute's 2025 NSS holds that, "the collaboration between America's internal and external subversive threats is unprecedented with authoritarian adversaries actively infiltrating and subverting most other countries that share American's democratic values." The NSS highlights strategic opportunities to identify common threats to renew or form new alliances.

Notable DoW efforts like the Defense Security Cooperation University have accomplished many successes, assisting several nations build their cyber commands and other capabilities including Presidential level policy that helped nations across the globe define their critical infrastructure.

CISA and other Executive agencies have proven examples of bilateral cooperation in cybersecurity and information sharing along with more regionalized initiatives that have opportunity to expand, such as the NATO Cyber Security Center.

One proposal that could leverage adversary cyber as a common threat is expanding the scope of a U.S. National Emergency by invoking NATO Article 5. This U.S. backed policy action would initiate a renewed transatlantic partnership for collective cyber defense against adversary cyber, meaning that an attack, pre-positioning, or cyber compromise against one Ally is considered an attack or compromise against all Allies. Further Cyber Diplomacy initiatives could continue to be led by the DOS Bureau of Cyberspace and Digital Policy and other efforts like the Diplomatic Security Service Directorate of Cyber and Technology Security.[37]

RECOMMENDATION: The ONCD, in collaboration with NIST National Cybersecurity Center of Excellence, DHS (including CISA), DoW, and the National Guard Bureau, develop ISAC program and framework that expands AI-security threat information with traditional CTI.

- Review past federally funded programs like the Center for Internet Security (CIS) Multi-State ISAC as a baseline. The initial goal of the MS ISAC was to be a focal point for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments. With the MS-ISAC emphasis on election security, the goodwill intent of the CIS model may require re-assessment to ensure goals are in-synch with America's best interests and national security. Without re-assessment, an entity like the MS-ISAC may have been used to support political interference in U.S. elections like was witnessed from China in 2020.
- Other assessments include the National Council of ISACs, which include Member groups designed by sector, such as the Aviation ISAC. Evaluate these ISACs and effectiveness or use with existing SRMA program and entities. A new ISAC framework must explore incentives for private industry to be stakeholders, not just members of an ISAC.
- Explore new models that could replace and purify an MS-ISAC, such as the use and designation of the National Guard Adjutant General as a dual hatted TAG and State Cyber Director (Commander) of the ISAC in each of the 50 states, under the National Emergencies Act. EXAMPLE: VA-ISAC for Virginia. The TAG, through the State CIO/CISO would also be responsible for the development of mandated state cyber strategy, risk management plan, and incident response policy. This would also enable international cooperation in cybersecurity by leveraging the National Guard State Partnership Program where states are engaged with selected foreign partners in common capability areas to include cybersecurity.

The development of a State-run ISAC program directly supports recommendations from the 2024 DSB Study on "DoD Dependencies on CI," to normalize engagement between installation commanders and civilian infrastructure owners. Enabling activities could include:

- Assign DoD points of contact for key infrastructure sectors with authority to commit to necessary actions or agreements and better communicate infrastructure protection issues to inform collection, analysis, and offensive action.

Pillar V. Defend and Leverage Emerging Technologies and Innovation to Advance Capabilities in Cyberspace

The Next Big Cyber Threat from Quantum Computers…Is the Government Ready?

The headline is based on a 2024 GAO Study where experts predicted that a quantum computer capable of breaking certain cryptography, referred to as a cryptographically relevant quantum computer (CRQC), may be developed in the next 10 to 20 years, putting agency and CI systems at risk. Federal agencies and our nation's CI, including energy, transportation systems, communications, and financial services are all dependent on technology systems and electronic data to provide essential services as well as to process, maintain, and report vital information.

Agencies along with CI owners and operators rely on cryptography (e.g., encryption) to protect sensitive systems and data. However, the emergence of quantum computers could undermine the security of widely used cryptographic methods.[38]

The Risks of Uncertainty

A 2024 CISCO Cyber Threat Trends Report highlights the most active cyber threats and technologies, all of which were used and identified with adversary cyber activities in a recent House Committee on Homeland Security "Cyber Threat Snapshot."[39] These included use of Information Stealers[iii], Trojans[iv], and Ransomware[v] to exploit vulnerabilities in both public and private sector networks for the purpose of personal theft (including financial), espionage, disruption, and strategic pre-positioning.

According to the House Committee report, advanced adversary cyber tactics used stealthy remote access trojans (or RATs), advanced APTs that could have been pre-positioned by ransomware, and botnets. Examples included:

- **HiatusRAT.** Suspected PRC-linked threat actor that targeted a U.S. military procurement system and Taiwan-based organizations. The threat gained access via pre-built malware samples which were hosted on virtual private servers. It is suspected the threat actor may have been gathering public information about military requirements or searching for associated organizations.
- **Cyber Av3ngers.** Iranian affiliated APT infiltrated Israeli software used in U.S. water and wastewater facilities in the wake of the October 7 Hamas terrorist attacks. The group accessed a component that regulates water pressure at a water authority in Pennsylvania, forcing the facility to utilize manual controls.
- **DarkSide.** Suspected Russian speaking affiliated "ransomware-as-a-service" group attacked Colonial Pipeline's IT systems, accessing just one password due to a lack of multifactor authentication in an older virtual private network. The company, which provides fuel to large parts of the country, was forced to halt business operations, causing serious disruptions in consumer access to fuel and an increase in price. Around 100 gigabytes of the company's data was held for a ransom of 75 bitcoin, or about $5 million. In June 2021, the DOJ seized $2.3 million worth of bitcoin from the threat actor.[40]
- **FlaxTyphoon.** PRC-affiliated botnet that burrowed into "IoT" consumer products such as cameras and network-connected storage devices to conduct espionage on strategic organizations in Taiwan, as well as organizations on U.S. soil through the telecommunications sector, media companies, and higher education institutions.

Consistent threat assessments, including ODNI and private sector cybersecurity reports forecast advances in adversary cyber and use of new advanced "enabler" technologies like AI. The threat grows

[iii] Malicious programs designed to collect various kinds of personal and financial information from an infected system. They can capture keystrokes, extract files, steal browser data like passwords and cookies, and more. Information stealers generate large amounts of DNS traffic, given that the threat exfiltrates data from a compromised organization.
[iv] Malware that misleads users of their true intent. They are often disguised as legitimate software; another common installation tactic is when a user gets a malicious link, like an email attachment disguised as an invoice, that once clicked on can silently install a Trojan. Once activated, they can enable cybercriminals to spy on you, steal your sensitive data, and gain backdoor access to your system.
[v] Malware that encrypts the files on a victim's computer or network, making them inaccessible, and demands a ransom payment to decrypt them. Victims are often threatened with permanent loss of data or exposure of stolen data if the ransom isn't paid.

across the AIE when combined in a hybrid environment, such as for electronic warfare or device network attacks. The attempted sim card network attack recently discovered by the U.S. Secret Service in New York City is an example of this hybrid conflict. According to officials, the network had the capability of carrying out a wide-range of telecommunications attacks — including spamming networks with up to 30 million text messages a minute — that could have had "catastrophic" consequences for the city, crippling cell towers and jamming 911 calls.[41]

Leverage Knowledge of Cyber Threats to Expedite Zero Day Solutions Across the AIE

As threats and AIE vulnerabilities increase, American cybersecurity solutions try to keep pace, with one example being the development of MITRE ATLAS that adds machine learning access and attack staging as adversary cyber framework techniques. [vi]

The 2025 AI Action Plan has already provided the groundwork, with several policy actions that can integrate implementation of **National Cyber Security Strategy** goals. These include promotion of secure-by-design principles and modification of incident and vulnerability response playbooks to incorporate AI and other future technologies. Implemented strategically, certain goals can be developed with existing CISA guidance like TECH strategy clusters and the Zero Trust Maturity Model, which assumes breach relies on, "never trust, always verify" rules and standardized IT architecture.[42]

RECOMMENDATION: Managed collaboratively between the Defense and Intelligence Advanced Research Projects (DARPA and IARPA), develop a National Digital Domain Range environment to test against threats to the AIE and advance science, research and development for new technologies, including smart city infrastructures.

- The Range environment can leverage existing organizations and infrastructures that might still be operational like the DoW National Cyber Range Complex and Smart City IoT Innovation efforts initiated by DHS Science & Technology for First Responders.
- Goal for an enhanced National Range capabilities that can begin to implement initial policy actions identified in the 2025 AI Action Plan and that could be identified in the National AI R&D Strategic Plan, support establishment of an AI & Autonomous System Virtual Proving Ground for military, test for data center vulnerabilities, and optimization of electrical grid to create a America First Energy Strategy Blueprint for the 21st Century.
- In addition to the development of a physical Range environment, explore the formation of National Digital Domain Range Association that can incorporate and offer an exchange for information across public and private sectors like the IBM X-Force Cyber Range and Texas A&M Institute of Data Science Digital Twin Lab (as two examples). A model is the Association of Research Parks that could be initiated through a group like the National Governors Association.

[vi] ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems) is a globally accessible, living knowledge base of adversary tactics and techniques against Al-enabled systems based on real-world attack observations and realistic demonstrations from Al red teams and security groups - atlas.mitre.org

RECOMMENDATION: In support of new 2025 AI Action Plan recommendations, ONCD lead in collaboration with White House Director of S&T Policy, NIST and the greater S&T community to prepare a report on the need for Congressional-level technology assessment organization.

- One CSC recommendation called for the re-establishment of The Office of Technology Assessment (OTA) that was created in 1972. The OTA produced assessments, background papers, technical memoranda, case studies, and workshop proceedings on a wide range of topics. Prior to defunding in 1995, many Members of Congress and outside observers found OTA's reports to be comprehensive, balanced, and authoritative; its assessments helped shaped public debate and laws in national security, energy, and health care. This could be replicated for an AIE and across USCI sectors.
- In 2018, Congress directed the CRS to work with the National Academy of Public Administration (NAPA) for a study to "assess the potential need within the Legislative Branch to create a separate entity charged with the mission of providing nonpartisan advice on issues of S&T.
    - The NAPA study recommended bolstering the S&T policy efforts of CRS and GAO, as well as the establishment of an Office of the Congressional Science and Technology Advisor (OCSTA) and a coordinating council. NAPA stated that it did not evaluate the option of reestablishing OTA due to Congress' efforts since 2002 to build a technology assessment capability within GAO.

Conclusion

We stand at the dawn of a new era – one that can redefine cybersecurity and shape the nation as a whole. As our country approaches its 250th birthday, the challenges before us are as complex as they are consequential.

Our 21st Century adversaries, international and domestic, will continue to plan, pre-position, and, in some instances, engage against the U.S. and foreign partners in cyberspace and greater AIE.

Some of the state-sponsored activity has traditional intents, like espionage to collect weapon system blueprints, but more groups are operating with the desire to inflict measurable disruption and spread disinformation to erode the Western ideals of God, family, country, and freedom.

As shocking as it sounds, this dangerous adversary even exists in our own chambers of Congress and on our Western Hemisphere borders. This internal threat requires some shift in national security strategy and thinking – away from the strategy of containment that defined the Cold War with the Soviet Union.

As we look across the sectors in the USCI, legacy equipment and risk management plans remain outdated and cyber hygiene becomes a stronger demand as the threat space grows in the AIE. This Blueprint isn't a solution, but rather a tool that can be used as a resource to further develop the **National Cyber Security Strategy** and propose efforts for a campaign to restore institutional trust in our federal government. This Blueprint also provides options for policymakers to consider that could impact

organization, operations, risk management, partnerships, and workforce development for cyber and digital transformation in the years to come.

We present this Blueprint with a clear understanding of the challenges ahead and a steadfast hope for a renewed "Morning in America." The security of our nation hangs in the balance—but through unity, innovation, and resolve, we can safeguard the ideals that define us, the great Republic, we proudly call the United States of America.

Glossary of Acronyms

AI: Artificial Intelligence – Techniques that simulate human intelligence, such as learning and problem-solving.

AIE: American Information Environment – Modeled after the military's definition of IE as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information-consisting of physical, informational, and cognitive dimensions.

APT: Advanced Persistent Threat – Sophisticated "full cycle" cyber tool or weapon used by adversary to access computer systems and networks.

CIP: Critical Infrastructure Program – Established by the North American Electric Reliability Corporation (NERC) to mitigate cybersecurity for America's bulk electric system. NERC CIP Reliability Standards apply to other CI entities like transportation, telecommunications, and financial services.

CISA: Cybersecurity and Infrastructure Security Agency – Agency under the Department of Homeland Security responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against adversary cyber.

CNMF: Cyber National Mission Force – Under U.S. Cyber Command, as part of Cyber Mission Force, responsible for defending the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.

CSC: Cyberspace Solarium Commission

CTI: Cyber Threat Intelligence

DEI: Diversity, Equity, and Inclusion – Politically influenced partisan discriminatory government program and policy that does not adhere to U.S. constitutional values and framework. Designated as illegal under Presidential Executive Order for, "Ending Radical and Wasteful Government DEI Programs and Preferencing," January 20, 2025.

DHS: Department of Homeland Security

DIB: Defense Industrial Base

DOJ: Department of Justice

DOS: Department of State

DoW: Department of War, formerly Department of Defense

DSB: Defense Science Board – Key advisory body established in 1956 to address complex national security challenges for the U.S. DoW.

EO: Executive Order – White House Presidential Directive.

FBI: Federal Bureau of Investigation

FCEB: Federal Civilian Executive Branch

GAO: Government Accountability Office – Independent, nonpartisan agency of the USG that provides auditing, evaluative, and investigative services for Congress – often referred to as the "congressional watchdog" to examine how taxpayer dollars are used and ensuring accountability and integrity in federal spending.

IT: Information Technology – The use of computers and telecommunications to store, retrieve, and transmit data.

IoT: Internet of Things

ISAC: Information Sharing and Analysis Center

NCF: National Cyber Force – Established in 2020 as the UK's partnership between defense, intelligence, and science and technology.

NCIRP: National Cyber Incident Response Plan

NIPP: National Infrastructure Protection Plan

NIST: National Institute of Standards and Technology

OT: Operational Technology – Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. OT describes environment containing industrial control systems like supervisory control and data acquisition (SCADA), distributed control system (DCS), remote terminal units (RTU), and programmable logic controllers (PLC).

PPD: Presidential Policy Directive

PRC: People's Republic of China – The official name of China's one-party state led by the ruling Chinese Communist Party.

SLGCP: State and Local Cybersecurity Grant Program

SLTT: State, Local, Tribal, and Territorial – Term used to describe local entities (outside of federal) who are responsible for ensuring the security of their jurisdictions, such as critical infrastructure and emergency preparedness.

SRMA: Sector Risk Management Agencies – Defined under Title 6, U.S. Code § 665d, they provide specialized sector-specific expertise to and support programs and associated activities for critical infrastructure owners and operators within its designated USCI sector or subsector.

USCI: U.S. Critical Infrastructure – 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

ZTA: Zero Trust Architecture – Security framework that continuously verifies all users and devices before granting access to resources, regardless of their location or network. Unlike traditional security models that assume everything within an organization's network is trustworthy, ZTA operates on the principle, "never trust, always verify."

Bibliography

[1] Federal Register. *Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*. Vol. 90, No. 60, March 31, 2025. Authorities under U.S. Code, Title 50, Chapter 34, "War and National Defense," §1622. National emergencies.
[2] Department of Defense. *Quadrennial Defense Review Report*. September 30, 2001.
[3] Flynn, Michael T. and Lovinger, Adam. *The Gold Institute for International Strategy National Security Strategy*. July 30, 2025.
[4] Radauskas, Gintaras. *Report: Lockbit, Qilin, DragonForce Join Forces as Ransomware Cartel*. Cybernews, October 10, 2025.
[5] Cilluffo, Frank (Task Force Chair). *Code Red: A Guide to Understanding China's Sophisticated Typhoon Cyber Campaigns*. McCrary Institute for Cyber and Critical Infrastructure Security Issue Brief, October 2025.
[6] U.S. Government Accountability Office (GAO). *Cybersecurity: An Overview of Cyber Challenges Facing the Nation, and Actions Needed to Address Them*. www.gao.gov/cybersecurity
[7] The White House. *Winning the Race: America's AI Action Plan*. July 2025.
[8] IBM Report. *Cost of Date Breach Report 2025: The AI Oversight Gap*. 2025.
[9] Identify Theft Resource Center Report. *2024 Data Breach Report*. January 2025.
[10] The White House. *National Cyber Workforce and Education Strategy: Initial Stages of Implementation*. June 25, 2024.
[11] U.S. GAO. *Information Environment: Opportunities and Threats to DoD's National Security Mission*. GAO-22-104714, September 2022.
[12] Auburn University McCrary Institute for Cyber and Critical Infrastructure Security. *Presidential Transition Task Force Report*. 2024.
[13] Department of Homeland Security, Cybersecurity and Critical Infrastructure Security Agency (DHS CISA). *Strategic Plan FY2024-2026*. www.cisa.gov/cybersecurity-strategic-plan
[14] The White House. *National Cybersecurity Strategy*. March 2023.
[15] Department of Defense. *2023 Cyber Strategy Summary*.
[16] Yang, Catherine. *As CCP Cybersabotage Escalates, US Changes Posture*. August 14, 2025.
[17] ODNI National Intelligence Council Assessment. *Cyber Operations Enabling Expansive Digital Authoritarianism (REDACTED)*. NICA 2020-027, April 7, 2020.
[18] The White House. *National Cyber Strategy of the United States of America*. September 2018.
[19] DHS CISA. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Alert AA24-038A, February 7, 2024.
[20] Department of Defense. *2018 Cyber Strategy Summary*.
[21] Montgomery, Mark and Lonergan, Erica. *United States Cyber Force: a Defense Imperative*. Foundation for Defense of Democracies, March 25, 2024.
[22] Switzer, Robert and Theohary, Catherine A. *Defense Primer: U.S. Cyber Command (USCYBERCOM)*. CRS In Focus report, IF 13042, June 25, 2025.
[23] Council on Foreign Relations. *What do the Trump Administration's Changes to PPD-20 Mean for Offensive Cyber Operations?* Contributions from Net Politics (Borghard and Lonergan), September 128, 2018.
[24] DHS CISA. *Joint Guidance: Identifying and Mitigating Living Off the Land Techniques*. February 7, 2024.
[25] DHS CISA. *PRC State-Sponsored Cyber Actor Living off the Land to Evade Detection*. Alert AA23-144A, May 24, 2023.
[26] Defense News Aerospace 2025. *China and Thailand Deepen Military Ties with Falcon Strike 2025 Joint Air Force Exercise*. September 17, 2025.
[27] Israel National News. *Iran: Cyberattacks Damage Critical Infrastructure During Operation Rising Lion*. July 22, 2025.

[28] Haynes, Deborah. *Iran's Alleged Secret Cyber Files Revealed.* Sky News, July 26, 2021.
[29] U.S. GAO. *Cyber Workforce: Actions Needed to Improve Size and Cost Data*. GAO-25-107405, September 4, 2025.
[30] CompTIA. *State of the Tech Workforce.* March 2025.
[31] U.S. GAO. *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight.* GAO-23-106415, January 19, 2023.
[32] U.S. GAO. *Cybersecurity High-Risk Series: Challenges in Securing Federal Systems and Information.* GAO-23-106428, January 31, 2023.
[33] U.S. GAO. *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure*. GAO-23-106441, February 7, 2023.
[34] U.S. GAO. *Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data*. GAO-23-106443, February 14, 2023.
[35] Gartner Press Release. *Gartner Identifies the Top Cybersecurity Trends for 2025.* March 3, 2025.
[36] Jaikaran, Chris. *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions.* CRS In Focus report, IF 12959, April 8, 2025.
[37] U.S. GAO. *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities.* GAO-24-105563, January 11, 2024.
[38] U.S. GAO. *Future of Cybersecurity: Leadership Needed to Fully Define Quantum Threat Mitigation Strategy.* GAO-25-107703, November 21, 2024.
[39] The U.S. House Committee on Homeland Security Press Release. *NEW: House Homeland Releases "Cyber Threat Snapshot" Highlighting Rising Threats to US Networks, Critical Infrastructure*. November 12, 2024
[40] U.S. Department of State Press Release. *Transnational Organized Crime Rewards Program: DarkSide Ransomware as a Service (RaaS)*. November 4, 2021.
[41] Marino, Joe and Crane, Emily. *Secret Service foils plot to cripple NYC cell network, threaten UN General Assembly.* New York Post, September 23, 2025.
[42] DHS CISA. *Zero Trust Maturity Model.* April 11, 2023.

Additional sources for recommendations:

- Pomerleau, Mark. *Congress Pushing Joint Task Force-Cyber, Shaking Up How DoD Employs Digital Capabilities.* DefenseScoop, July 24, 2025.
- Defense Science Board. *Executive Summary: Future Cyber Warfighting Capabilities.* May 2024. *and DoD Dependencies on Critical Infrastructure (August 2024).*
- Defense Science Board. *Executive Summary: DoD Dependencies on Critical Infrastructure.* August 2024.
- Joint DoD/DHS Report. *NIPP Annex: Defense Industrial Base Sector-Specific Plan.* 2010
- U.S. House. *Cyber PIVOTT Act – Proving Individuals Various Opportunities for Technical Training to Build a Skills-Based Cyber Workforce.* 118th Congress, H.R. 9770, Introduced September 24, 2024.
- DHS CISA. *Guidance: Cybersecurity Best Practices for Smart Cities.* April 19, 2023
- Blevins, Emily. *The Office of Technology Assessment: History, Authorities, Issues, and Options.* CRS Report No. R46327, April 29, 2020.

Blueprint for National Cyber Security Strategy Advisory Review Contributors:

Herm Hasken, CEO & Senior Advisor, High Ground Advisors
Katie Kenlein, Executive Assistant, The Gold Institute for International Strategy
Dr. Christopher Porter, Head of International Security, Google
Nick Rocha, Founder and CEO, Neptune SHIELD Tech Hub

ON BEHALF OF:

Chairman of the Board
The Gold Institute for International Strategy
Honorable Michael T. Flynn
Lieutenant General, U.S. Army (Retired)

President of The Gold Institute for International Strategy
Eli M. Gold

We wish to thank our roundtable sponsors for supporting our combined efforts crafting this Blueprint to assist and inform strategy, policy, operations, risk management, and partnership for cyber and digital transformation.

Contact us:

The Gold Institute for International Strategy
www.goldiis.org

Cyber Intelligent Partners LLC
www.cipsolutions.tech