2024 Report on the Cybersecurity Posture of the United States

MAY 2024

OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE OFFICE OF THE PRESIDENT

THE WHITE HOUSE
WASHINGTON

About This Report

The National Cyber Director is providing this report to the President, the Assistant to the President for National Security Affairs, and Congress as required under 6 U.S.C. § 1500 (c)(1)(C)(vi). This report assesses the cybersecurity posture of the United States, the effectiveness of national cyber policy and strategy and the status of the implementation of national cyber policy and strategy by Federal departments and agencies. As defined in 6 U.S.C. § 1500 (g)(1), the term "cybersecurity posture" means the ability to identify, to protect against, to detect, to respond to, and to recover from an intrusion in an information system the compromise of which could constitute a cyber attack or a cyber campaign of significant consequence.

In addition, and as required under 6 U.S.C. § 1500 (c)(1)(G), this document reports to Congress on cybersecurity threats and issues facing the United States, including any new or emerging technologies that may affect national security, economic prosperity, or enforcing the rule of law.

This report focuses on events that occurred during the past year and addresses earlier events as necessary to provide context.

★ ★ ★ ★ ★ ★

Letter from the National Cyber Director

I am pleased to present the *2024 Report on the Cybersecurity Posture of the United States*. This first-ever report provides important updates on how the Nation is addressing the challenges and opportunities we face in cyberspace. We have made progress in realizing an affirmative vision for a safe, prosperous, and equitable digital future, but the threats we face remain daunting, our defenses are not impregnable, and our work continues to evolve to meet the changing landscape.

Simply put, we are in the midst of a **fundamental transformation** in our Nation's cybersecurity. It is now clear that a reactive posture cannot keep pace with fast-evolving cyber threats and a dynamic technology landscape, and that aspiring just to manage the worst effects of cyber incidents is no longer sufficient to ensure our national security, economic prosperity, and democratic values. Beginning with Executive Order 14028 on *Improving the Nation's Cybersecurity*, the Biden-Harris Administration has advanced an affirmative vision centered on proactively and strategically shaping the digital world around us, positioning it to enable every aspect of our economy and society.

The President's National Cybersecurity Strategy asserts that it is necessary to fundamentally shift the underlying dynamics of the digital world to make it defensible, resilient, and aligned with our values. If we succeed, the digital ecosystem can be a strong foundation for a prosperous, connected future that benefits every American. While we remain postured to forcefully respond to malicious cyber threats, we will not let our adversaries dictate our path forward.

Implementing this new vision requires a collaborative, whole-of-nation effort. The most capable and best-positioned actors in cyberspace, in both public and private sectors, need to do more to reshape the digital ecosystem and protect the vulnerable. We are committed to working closely with our partners in the private sector, with State, local, Tribal, and territorial entities, and with like-minded nations around the world to enhance our collective resilience to cyber threats.

Congress has also been a vital partner in this implementation process, and we will continue to engage with Congress to ensure that departments and agencies have the resources and authorities they need. With no shortage of challenges on the horizon, the Administration and Congress must continue to work together in a nonpartisan manner to advance U.S. cybersecurity and resilience.

As the President stated at the Strategy's launch, "The steps we take and choices we make today will determine the direction of our world for decades to come." We need to build on the successes of the past year, learn lessons from where we fell short, and take on hard challenges such as harmonizing cybersecurity regulations, empowering Sector Risk Management Agencies, and supporting smaller organizations facing down capable adversaries. Together, we will build a digital world that keeps Americans safe from cyber threats and enables our grandest ambitions.

Harry Coker, Jr.
National Cyber Director

Executive Summary

The *2024 Report on the Cybersecurity Posture of the United States* assesses the cybersecurity posture of the United States, the effectiveness of national cyber policy and strategy, and the status of the implementation of national cyber policy and strategy by Federal departments and agencies. Additionally, this report highlights cybersecurity threats and issues facing the United States, including new or emerging technologies that may affect national security, economic prosperity, and the rule of law. This is the first edition of the report and covers calendar year 2023, with additional consideration of developments in 2024 preceding the publication of this report.

Over the past year, U.S. national cybersecurity posture improved, driven by steady progress towards the 2023 National Cybersecurity Strategy's (NCS) vision of a defensible, resilient, and values-aligned digital ecosystem achieved through fundamental shifts in the underlying dynamics that shape cyberspace. The Administration has successfully begun implementation of the NCS Implementation Plan, which coordinates actions by departments and agencies across the Federal Government to make the President's affirmative vision a reality. These initial implementation actions set the foundation for further investment and sustained commitment by stakeholders across the digital ecosystem.

The Strategic Environment

This report begins with an assessment of the strategic environment, the landscape of emerging technologies and cyber risks that present both challenges and opportunities for U.S. cybersecurity policy and strategy. The analysis of emerging technologies considers not just their internal technical characteristics, but also their integration into complex systems and processes, their connection to people and workers, and their relationship to institutions and governance structures. This report also examines the cyber risk landscape, considering both trends in threat actor capability and intent, as well as the evolving vulnerabilities in our own defenses that create pathways for these adversaries to exploit.

In 2023, the strategic environment was characterized by **complexity**, **interconnectivity**, and **competition**. Continued progress in digital communications, advanced computing, quantum information science, data storage and processing, and other critical and emerging technologies are rapidly increasing the complexity of our economy and society. These technologies also connect people around the world, enable the proliferation of cyber-physical systems, and create new dependencies between critical infrastructure and essential services across every sector. As this landscape evolves, malicious state and non-state actors are exploiting its seams with growing capability and strategic purpose, making clear that cyberspace is closely aligned with other domains of international conflict and competition.

★ ★ ★ ★ ★ ★

Five trends, in addition to enduring cybersecurity challenges, drove change in the strategic environment in 2023.

1. **Evolving Risks to Critical Infrastructure**: Nation-state adversaries demonstrated a growing willingness to use cyber capabilities to compromise and hold at risk critical infrastructure systems and assets with no inherent espionage value, in order to further their broader strategic objectives.

2. **Ransomware**: Ransomware remained a persistent threat to national security, public safety, and economic prosperity, and ransomware groups continued to develop sophisticated strategies to evade or circumvent defensive and disruptive measures designed to frustrate their activities.

3. **Supply Chain Exploitation**: Complex and interconnected supply chains for software and other information technology and services enabled malicious actors to compromise victims at scale.

4. **Commercial Spyware**: There was a growing market for sophisticated and invasive cyber-surveillance tools sold to nation-state actors by private vendors to access electronic devices remotely, monitor and extract their content, and manipulate their components without the knowledge or consent of the devices' users.

5. **Artificial Intelligence**: Artificial intelligence (AI) is one of the most powerful, publicly accessible technologies of our time, and its continued evolution in 2023 presented opportunities and challenges for cyber risk management at scale.

Current Efforts

Addressing the challenges and seizing the opportunities presented by the strategic environment requires a coherent program of action led by the Federal Government and aligned with private sector efforts. The Office of the National Cyber Director (ONCD) coordinates the implementation of national cyber policy and strategy, including the NCS, by driving new actions and uplifting and connecting work underway. This report reflects important contributions to national cybersecurity made by departments and agencies across the Federal Government.

The National Cybersecurity Strategy Implementation Plan (NCSIP), released in July 2023, guides Federal efforts to realize the vision of the NCS and is updated on an annual basis. In NCSIP Version 1, the Federal Government was responsible for completing 36 initiatives by the second quarter of 2024. As detailed in this report, 33 of these 36 (92%) initiatives were completed on time and three remain underway. An additional 33 NCSIP Version 1 initiatives have completion dates over the next two years and are on track.

★ ★ ★ ★ ★ ★

Actions taken by the Federal Government during the period covered by this report include:

1. **Establishing and Using Cyber Requirements to Protect Critical Infrastructure**, including through the development and harmonization of regulatory requirements in multiple critical infrastructure sectors.

2. **Enhancing Federal Cooperation and Partnerships** to better support cyber defenders, including by increasing operational collaboration, improving Sector Risk Management Agency (SRMA) capacity, and integrating Federal cyber defense capabilities.

3. **Improving Incident Preparedness and Response** by rapidly sharing threat information, prioritizing support to victims, and reviewing significant incidents and campaigns to derive lessons learned.

4. **Disrupting and Degrading Adversary Activity** using all tools of national power, resulting in coordinated, high-impact disruption campaigns against a wide range of malicious cyber actors.

5. **Defending Federal Networks** at speed and scale, including by integrating Zero Trust Architecture principles across the Federal enterprise, modernizing legacy technology systems, and expanding the use of shared services.

6. **Strengthening the National Cyber Workforce**, including through the promulgation of a National Cyber Workforce and Education Strategy (NCWES) and engagement with workers, employers, students, and educators across the country.

7. **Advancing Software Security to Produce Safer Products and Services**, including by advancing Secure by Design principles, Software Bills of Material (SBOM), and memory-safe programming languages.

8. **Enabling a Digital Economy that Empowers and Protects Consumers**, including by launching a U.S. Cyber Trust Mark certification and labeling program and by promoting competition and accountability across the technology industry.

9. **Investing in Resilient Next-Generation Technologies** across the clean energy economy, issuing an executive order to guide Federal efforts related to artificial intelligence, and addressing security challenges present in the technical foundations of the Internet.

10. **Managing Risks to Data Security and Privacy** by enabling safe, data-rich cross-border commerce and promoting the development of privacy-enhancing technologies.

11. **Enhancing Resilience Across the Globe** by building coalitions of like-minded nations to provide support to victims of ransomware and other cyberattacks, align national policy, and promote secure and resilient global supply chains.

★ ★ ★ ★ ★ ★

12. **Advancing a Rights-Respecting Digital Ecosystem** by advancing an affirmative vision of an open, free, global, interoperable, reliable, accessible, and secure Internet; combatting the proliferation and misuse of digital technologies like commercial spyware; and shaping emerging technologies to align with democratic values and human rights.

Future Outlook

In 2024 and beyond, the Federal Government will build on accomplishments of the past year, continue to implement the NCS and NCWES, and adapt its approach to address emergent challenges and opportunities presented by an evolving strategic landscape. It will be necessary to sustain efforts to enhance the capabilities of Sector Risk Management Agencies, strengthen the national cyber workforce, implement incident reporting requirements directed by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), enhance the speed and scale of adversary disruption campaigns, improve analytics and information sharing mechanisms, continue to invest in quantum information science, and prioritize cybersecurity in foreign assistance mechanisms.

The next iteration of the NCS implementation plan, NCSIP Version 2, outlines 31 new initiatives that build on shared accomplishments of the past year and establish new lines of effort to continue to implement the NCS. NCSIP Version 2 has been published alongside this report and is available online at www.whitehouse.gov/oncd.

★ ★ ★ ★ ★ ★

TABLE OF CONTENTS

★ ★ ★ ★ ★ ★

Introduction

A fundamental transformation is underway. At the core of this transformation are new technologies which we have made foundational to our national security, our economy, our democracy, and our modern way of life. Innovations in the fields of Artificial Intelligence (AI), quantum information science (QIS), and microelectronics are revolutionizing the advanced computing landscape. Our digital and physical worlds are increasingly connected, in both industrial applications and consumer-facing products. Growing access to high-speed Internet and the proliferation of next-generation telecommunications networks are connecting people and systems around the world.

As this digital ecosystem evolves, our adversaries have repeatedly demonstrated their capability and intent to exploit its vulnerabilities. Both state and non-state actors continue to aggressively conduct malicious cyber activity that threatens U.S. national security, public safety, and economic prosperity. Critical infrastructure across the United States has been held at risk by the People's Republic of China (PRC) and other adversaries who threaten our essential services and public safety in service of their geopolitical ambitions. Ransomware groups have built a business model around targeting schools, hospitals, small businesses, and many others ill-equipped to defend themselves.

In this decisive moment, the Biden-Harris Administration put forth a new approach centered on proactively shaping our shared, digitally-enabled future. Released in March 2023, the President's National Cybersecurity Strategy (NCS) articulates a new, affirmative vision of a digital ecosystem that is defensible, resilient, and aligned with our values. The NCS moves away from previous approaches that were predicated on managing threat actors in a digital ecosystem that advantaged their malicious activity. Instead, the NCS calls for two fundamental shifts in how we allocate roles, responsibilities, and resources in cyberspace by (1) rebalancing the responsibility to defend cyberspace away from end users and to the most capable and best-positioned actors in the public and private sectors, and (2) realigning incentives to favor long-term investments in future resilience.

The NCS recognizes the need for modern and nimble regulatory frameworks for critical infrastructure cybersecurity. The NCS targets market interventions, such as device labeling programs and a software liability regime, to address economic dynamics that contribute to poor cybersecurity outcomes. Where technical vulnerabilities create pervasive challenges for cyber defenders, the NCS calls for coordinated investment in standards and research and development to eliminate them. And, as the NCS makes clear, investing in talent is a key part of investing in our digital future. The 2023 National Cyber Workforce and Education Strategy (NCWES) outlines a comprehensive approach aimed at addressing both immediate and long-term cyber workforce needs while empowering every American to participate in our digital ecosystem.

With this new strategic course set, the Administration has turned to the vital work of implementation. Successful implementation is at its core a collaborative endeavor, requiring contributions from across the Federal Government, industry, academia, civil society, and other partners around the world. Congress has provided essential support to the implementation process by empowering departments and agencies with necessary authorities and resources.

★ ★ ★ ★ ★ ★

Version 1 of the NCS Implementation Plan (NCSIP) lays out a roadmap of 69 initiatives for the Federal Government to carry out to achieve the NCS's objectives. To date, the cybersecurity community has completed 33 items in the first year of the NCSIP, and undertaken countless other efforts to make cyberspace safer and more secure. The next iteration of the NCSIP, Version 2, builds on successes achieved in the first year of implementation, responds to emerging and unexpected challenges, and outlines 31 new initiatives to implement the 2023 NCS. This report highlights key implementation efforts, accomplishments, and trends from the past year to demonstrate how the United States is proactively and strategically shaping the digital ecosystem to make it more defensible, resilient, and aligned with our values.

★ ★ ★ ★ ★ ★

The Strategic Environment

The strategic environment consists of an evolving ecosystem of people, technologies, and institutions, as well as the malicious actors who exploit vulnerabilities in this ecosystem to cause harm. The Office of the Director of National Intelligence's *2024 Annual Threat Assessment of the U.S. Intelligence Community* makes clear that both state and non-state actors continue to pursue cyber capabilities that threaten U.S. national interests in cyberspace and beyond. The PRC, in particular, remains the most active and persistent cyber threat to U.S. Government, private sector, and critical infrastructure networks. Nation-state actors from Russia, Iran, and the Democratic People's Republic of Korea (DPRK), as well as transnational criminal organizations and other non-state actors, are responsible for a wide range of malicious activity that impacts the United States and our allies and partners.

However, the cyber risk landscape is defined by more than these actors and their malicious activities. Threat is only one component of risk, and remedying vulnerabilities in cyberspace, enhancing our resilience, or otherwise mitigating the consequences of successful cyber incidents are more directly within our control. In analyzing the strategic environment, this report considers the combination of adversary capability and intent, the distribution and severity of vulnerabilities in our digital ecosystem, and the processes and policies we deploy to address these challenges. Below, we highlight both enduring cybersecurity challenges and the emergent trends that drove change in the strategic environment this year.

Our strategic environment is characterized by growing **complexity**, **interconnectivity**, and **competition**, as critical and emerging technologies further accelerate the pace of change and require us to rapidly reimagine risks and opportunities in a digitally-enabled world. Advanced computing technologies, the convergence of digital and physical systems, and the presence of new actors across our critical infrastructure landscape make for a complex world where risks can be difficult to identify. Sprawling supply chains, widening access to communications networks, and interdependent global infrastructures have led to an increasingly interconnected world. Simultaneously, the strategic environment has become increasingly competitive, as both state and non-state actors pursue their interests using sophisticated cyber capabilities. Geopolitical conflict is increasingly playing out in cyberspace, amplifying risks to U.S. and allied critical infrastructure.

Enduring Cybersecurity Challenges

Cyber defenders face more adversaries than ever, as a growing number of state-affiliated, criminal, and ideologically-motivated actors launch cyber operations against the United States. These **adversaries benefit from longstanding structural asymmetries**, including the fact that attackers can begin exploiting vulnerabilities before defenders can develop and deploy patches, and network interdependencies that allow exploitation of victims at scale. Enduring use of insecure practices by the software development community, such as programming in memory unsafe languages, further advantages attackers. Additionally, challenges in attribution enable malicious actors to obfuscate their behavior to avoid consequences.

★ ★ ★ ★ ★ ★

Legacy protocols and technical architectures with poor security attributes are deeply embedded across the digital ecosystem, from legacy mobile networks to how we route data across the Internet. The Border Gateway Protocol (BGP), which directs Internet traffic, is susceptible to traffic hijacking and route manipulation. Attackers can also leverage weaknesses in outdated encryption protocols to compromise communications.

Emerging digital technologies often present adversaries with new opportunities for malicious exploitation. The development of a viable large-scale quantum computer, for example, promises tremendous economic benefits, potentially creating entirely new industries and revolutionizing our digital ecosystem. However, we have known for decades that quantum computing has the potential to break many widely used cryptographic systems that keep our information safe. In the wrong hands, a sufficiently mature quantum computer would challenge the integrity of the digital ecosystem, threaten sensitive health and personal financial data, and defeat security protocols for most Internet-based financial transactions.

Critical infrastructure owners and operators rely on **third-party service providers** to manage key aspects of their digital operations. The adoption of cloud services, for example, can enable better and more economical cybersecurity outcomes at scale, but cloud migration may also present novel cybersecurity risks. Hybrid deployments, in which organizations use both locally hosted systems and cloud assets, can introduce complex centralized logging and authentication regimes, creating opportunities for malicious actors to evade detection and abuse identity management systems. The 2023 PRC compromise of U.S. government communications demonstrates the necessity of maintaining comprehensive logging. More broadly, as organizations migrate increasing amounts of data and processes to the cloud, this shift introduces new cross-sector dependencies and complicates systemic risk identification and management, particularly where multiple organizations rely on third-party services from the same provider.

Our critical infrastructure landscape is characterized by **private ownership and operation**, which results in interdependencies between public and private sectors and which requires a national cybersecurity posture rooted in public-private action, collaboration, and partnership. The rapidly expanding space industry illustrates how advances in technology create new challenges and opportunities for collaboration to manage shared cyber risk. A growing number of critical infrastructure assets rely upon space-based systems for communications, sensing, navigation, and timing. In the days leading up to Russia's 2022 invasion of Ukraine, a cyberattack against a U.S. space communications company, ostensibly intended to disrupt Ukrainian telecommunications, also led to outages for computer systems used by thousands of European wind turbines. As the space ecosystem continues to evolve and integrate new commercial participants, the cybersecurity of space systems will be a shared responsibility.

America's **cyber workforce** continues to grapple with a persistent need for more trained cybersecurity professionals and a better cyber education ecosystem. Getting more Americans involved in the cyber workforce not only strengthens our national cybersecurity outcomes, it also provides access to good-paying, middle-class jobs. We must develop cyber talent through formal and informal cyber education and training systems as a matter of economic development and national security. While U.S. schools, governments, non-profits, and companies have made

strides in developing American cyber talent, these investments have lacked the scale and coordination necessary to meet increasing demand.

Top Trends of 2023

Evolving Risks to Critical Infrastructure

U.S. critical infrastructure faces evolving and unacceptable cyber risks. Nation-state adversaries are developing cyber capabilities and gaining accesses with the intent of disrupting or destroying U.S. and allied critical infrastructure. Such disruptions could support or enable an adversary's strategic objectives outside of the cyber domain and pose challenges for risk management within and across critical infrastructure sectors.

While adversaries pre-positioning for cyberattacks is a long-standing threat, the PRC's pre-positioning activity is a threat unlike any America has previously faced. In 2023, a PRC actor tracked as Volt Typhoon gained access to critical infrastructure in the United States and the Indo-Pacific region. Critically, this campaign targeted U.S. entities that presented little value from an espionage or intelligence perspective, but which could enable disruption of operational technology systems in critical infrastructure and interference with U.S. and allied warfighting capabilities. Also in 2023, PRC actors tracked as BlackTech used sophisticated tools to compromise routers and gain access to a wide variety of U.S. and Japanese critical infrastructure. These intrusions demonstrated the PRC's intention to hold at risk U.S. and allied critical infrastructure, shape U.S. decision-making in a time of crisis, and use cyber capabilities to augment PRC geopolitical objectives.

Ransomware

Ransomware remains a persistent threat to national security, public safety, and economic prosperity. Comprehensive data on the full scope of the ransomware threat is difficult to obtain, particularly with cyber incident reporting requirements still evolving and victims reluctant to share information about attacks. Following a brief decrease in 2022, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received a 22% increase in reported ransomware incidents from American victims. Reports to the IC3 also reflected a 74% increase in the cost of ransomware incidents in 2023, relative to 2022.

Established ransomware groups are continuing to develop sophisticated strategies to monetize their accesses and evade or circumvent defensive measures designed to frustrate their activities. Attackers have increased the use of "double" and "triple extortion" attacks, not only encrypting victims' data but also threatening to sell or publicly release that data if a ransom is not paid, and sometimes also threatening to dox victims if they do not pay an additional fee. Victims who make these additional ransomware payments rely on their attackers' promise to delete exfiltrated data and refrain from doxing attacks, a promise that is not always kept. Ransomware actors form conspiracies with each other, dividing up the work of developing and deploying malware, carrying out attacks on individual targets, and collecting cryptocurrency ransoms. This form of criminal economic specialization has made the ransomware threat especially potent.

★ ★ ★ ★ ★ ★

Supply Chain Exploitation

Complex and interconnected supply chains for software and other information technology and services, combined with growing reliance on common third-party service providers, create opportunities for sophisticated adversaries to access victims at scale and complicate the efforts of defenders to identify and manage cybersecurity risks. Adversaries are increasingly taking advantage of complex and interconnected relationships between organizations and their suppliers, customers, vendors, and service providers, compromising single nodes that grant surreptitious access to victims in the United States and around the world.

In 2023, several high-profile compromises of technology providers impacted thousands of connected victims, including critical infrastructure owners and operators. In December, Russia's Foreign Intelligence Service (SVR) targeted servers used by computer programmers to compile and test software, presumably intending to maliciously modify developers' source code. Earlier in the year, a compromise of a widely used identity and access management firm enabled malicious actors to steal credentials and session tokens that could provide surreptitious access to thousands of customers. And, at the beginning of the year, a popular enterprise communications suite was compromised in an entirely separate supply chain attack, demonstrating how a single initial compromise can quickly spread through interlinked technology supply chains and third-party relationships.

Commercial Spyware

There is a growing market for sophisticated and invasive end-to-end cyber-surveillance tools sold by private vendors to access electronic devices remotely, monitor and extract their content, and manipulate their components without the knowledge or consent of the devices' users. Commercial spyware providers now offer world-class capabilities to the highest bidder, who often employ these capabilities in cyber operations that are not subject to oversight or regulatory constraints. While the commercial spyware industry has a long history, the recent proliferation and misuse of these tools allows malicious cyber actors to target journalists, activists, human rights defenders, and government officials with greater frequency.

A growing number of authoritarian regimes and democratic governments have misused commercial spyware to surveil targets; intimidate perceived opponents; suppress dissent; limit freedoms of expression, peaceful assembly, or association; and otherwise abuse human rights. Some foreign governments and persons have deployed commercial spyware against U.S. government personnel, information, and computer systems, presenting significant counterintelligence and security risks to the United States. The misuse of these tools also threatens the security and privacy of individuals in the United States and around the world.

Artificial Intelligence

Artificial intelligence (AI) is one of the most powerful technologies of our time, and it continues to receive substantial public attention and media coverage. Advances in large-language models (LLMs) and other foundational algorithms, combined with more affordable computing power and access to data, have given rise to a new generation of AI tools. These tools captured

the public's imagination in 2023, as Americans experienced novel applications such as chatbots and image generators. AI will almost certainly continue to evolve at a rapid pace in the years to come, with public and private entities around the world vying for profit and competitive advantage.

The evolving AI landscape will present cyber defenders with new opportunities to defend critical infrastructure against malicious activity. The cybersecurity community has a long history of harnessing the power of machine learning techniques for basic tasks like data processing, email filtering, and malware identification. New cyber defense tools that integrate AI could eventually enable cyber defenders to more efficiently detect anomalous network traffic and other adversary activity, coordinate the defense of complex systems and networks, and augment a cybersecurity workforce that is already stretched thin.

AI tools may also make our software development ecosystem safer and more secure. While LLMs have shown some fluency in programming languages, they cannot yet generate commercially useful secure code without human intervention. Responsible integration of AI tools into the software development lifecycle may enable developers to identify vulnerabilities in new code and suggest potential fixes. As AI tools mature, they could be able to make widely used software products more secure by rewriting existing code into a memory-safe programming language.

However, realizing the promise of AI also challenges us to manage the risks it poses to cybersecurity. Today, LLMs can quickly and cheaply generate persuasive and micro-targeted text, images, audio, and video in different languages. Cybercriminals, hacktivists, and others with limited resources and technical sophistication may use these capabilities to conduct phishing campaigns, information operations, and other malicious cyber activity. AI-enabled surveillance and censorship technologies enable authoritarian regimes to more effectively and efficiently target journalists, dissidents, and human rights defenders. Without safeguards, AI technologies may also put Americans' privacy at risk by making it easier to extract, identify, and exploit personal data. As the AI ecosystem continues to evolve, there is an opportunity to ensure that its core elements—data, computing, and algorithms—are developed with safeguards against misuse.

★ ★ ★ ★ ★ ★

Current Efforts

The Federal Government is undertaking a bold program of action to implement the NCS and proactively shape the digital ecosystem to align with U.S. national objectives. These efforts build on generational investments in new infrastructure through the Bipartisan Infrastructure Law (BIL), Inflation Reduction Act (IRA), and CHIPS and Science Act; cybersecurity legislation such as CIRCIA; and executive actions including Executive Order (EO) 14028 on *Improving the Nation's Cybersecurity*, National Security Memorandum (NSM) 5 on *Improving Cybersecurity for Critical Infrastructure Control Systems*, and NSM-8 on *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Systems*.

NCSIP Version 1, released in July 2023, guides Federal efforts to realize the vision of the NCS through 69 high-impact initiatives, from combatting cybercrime to building a skilled cyber workforce to addressing security challenges present in the technical foundations of the Internet. In NCSIP Version 1, the Federal Government was responsible for completing 36 initiatives by the second quarter of 2024. As detailed in the table below, 33 of these 36 (92%) initiatives were completed on time and three remain underway. An additional 33 NCSIP Version 1 initiatives have completion dates over the next two years and are on track.

Alongside this report, ONCD has published NCSIP Version 2, which builds on successes achieved in the first year of implementation, responds to evolving challenges, and outlines 31 new initiatives to implement the 2023 NCS. Twenty-four agencies are leading initiatives in NCSIP Version 2, with six new agencies joining the implementation effort to achieve the vision of the NCS. Further details on progress made on initiatives in NCSIP Version 1 and ongoing and new initiatives in NCSIP Version 2 can be found online at www.whitehouse.gov/oncd.

NCS Implementation Progress

NCSIP Initiative	Initiative Title	Responsible Agency
1.1.1	Establish an initiative on cyber regulatory harmonization	ONCD
1.2.2	Provide recommendations for the designation of critical infrastructure sectors and sector risk management agencies	CISA
1.3.1	Assess the capabilities of Federal Cybersecurity Centers and related cyber centers	ONCD
1.4.3	Develop exercise scenarios to improve cyber incident response	ONCD
1.4.4	Draft legislation to codify the Cyber Safety Review Board with the required authorities	Homeland Security
1.5.1*	Develop an action plan to continue to secure unclassified Federal Civilian Executive Branch Systems	OMB
2.1.1	Publish an updated Department of Defense Cyber Strategy	Defense
2.1.4	Propose legislation to disrupt and deter cybercrime and cyber-enabled crime	Justice
2.1.5*	Increase the speed and scale of disruption operations	FBI
2.2.1	Identify mechanisms for increased adversarial disruption through public-private operational collaboration	ONCD

2.4.1	Publish a Notice of Proposed Rulemaking on requirements, standards, and procedures for Infrastructure-as-a-Service providers and resellers	Commerce
2.5.1	Develop an action plan to disincentivize safe havens for ransomware criminals	State
2.5.2	Increase the speed and scale of operations to disrupt ransomware crimes	FBI
2.5.3	Improve investigation of ransomware crimes	Justice
3.2.1	Publish a Notice of Proposed Rulemaking to change the Federal Acquisition Regulation in line with the Internet of Things Cybersecurity Improvement Act of 2020	OMB
3.2.2	Initiate a U.S. Government Internet of Things security labeling program	NSC
3.3.1	Explore approaches to develop a long-term, flexible, and enduring software liability framework	ONCD
3.4.1	Develop guidance for Federal agencies and grantees to better leverage Federal grants to improve infrastructure cybersecurity	ONCD
3.4.2	Include cybersecurity as a priority for research funding	OSTP
3.5.1*	Publish a Notice of Proposed Rulemaking to change the Federal Acquisition Regulation to incorporate new requirements outlined in Executive Order 14028	OMB
3.6.1	Assess the need for a Federal insurance response to a catastrophic cyber event	Treasury
4.1.1	Lead the adoption of network security best practices	OMB
4.1.2	Promote open-source software security and the adoption of memory safe programming languages	ONCD
4.1.3	Reinvigorate interagency coordination on international cybersecurity standards	NIST
4.2.1	Publish an updated cybersecurity research and development strategy	OSTP
4.4.1	Drive adoption of cyber secure-by-design principles by incorporating them into Federal projects	Energy
4.4.2	Develop a plan to ensure the digital ecosystem can support and deliver the U.S. Government's decarbonization goals	ONCD
4.6.1	Publish a National Cyber Workforce and Education Strategy and track its implementation	ONCD
5.1.2	Publish an International Cyberspace and Digital Policy Strategy	State
5.2.1	Improve interagency coordination to strengthen international partners' cyber capacity	State
5.3.1	Establish flexible foreign assistance mechanisms to provide cyber incident response support quickly	State
5.5.1	Promote the development of secure and trustworthy information and communication technology (ICT) networks and services	State
5.5.2	Promote a more diverse and resilient supply chain of ICT vendors	State
5.5.3	Begin administering the Public Wireless Supply Chain Innovation Fund	Commerce
6.1.2	Apply lessons learned to the National Cybersecurity Strategy implementation	ONCD
6.1.3	Publish budgetary guidance aligned with National Cybersecurity Strategy implementation	ONCD

** indicates initiatives in-progress as of date of publication*

★ ★ ★ ★ ★ ★

Establishing and Using Cyber Requirements to Protect Critical Infrastructure

The NCS calls for the use of incentives and requirements to align the interests of individuals and organizations with our collective goals of national security, public safety, and economic prosperity. The Federal Government's proactive approach to cybersecurity requirements recognizes that every sector must be accounted for. Where cybersecurity requirements do not exist or are poorly defined, we are pursuing new requirements that are agile enough to adapt as adversaries increase their capabilities and change tactics. Where the regulatory landscape is already mature, we are working to harmonize and align new and existing regulatory requirements. We are also paying close attention to regulatory action in other countries where such efforts can serve as a model, or where these actions may impact U.S. critical infrastructure owners, operators, or third-party service providers.

In the past year, new or updated cybersecurity rules went into effect across several critical infrastructure sectors. The Transportation Security Administration (TSA) issued updated requirements for oil and natural gas pipelines, airport and aircraft operators, and rail carriers. The Securities and Exchange Commission (SEC) adopted new rules requiring public companies to disclose information related to material cybersecurity incidents and risk management practices. In the healthcare and public health (HPH) sector, an amendment to the Federal Food, Drug, and Cosmetic Act, one of the Food and Drug Administration's (FDA) authorizing statutes, now requires manufacturers of certain types of medical devices to design, develop, and maintain cybersecure medical devices, including through the creation of comprehensive lists of software components. FDA also finalized updated recommendations for medical device manufacturers to comply with FDA rules related to medical device cybersecurity. For the Defense Industrial Base (DIB), the Department of Defense (DoD) released revisions to its Cybersecurity Maturity Model Certification program to establish new requirements for DIB contractors and sub-contractors and expanded access to the voluntary DIB Cybersecurity (CS) Program. And, in the maritime sector, the President signed EO 14116 on *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States* alongside the U.S. Coast Guard issuing a Maritime Security Directive and Notice of Proposed Rulemaking (NPRM) to bolster port and maritime cybersecurity.

Across all critical infrastructure sectors, implementation of CIRCIA will establish new requirements for covered entities to report certain cybersecurity incidents to the Federal Government. In March 2024, CISA published an NPRM setting out proposed regulations for cyber incident and ransom payment reporting, as well as other aspects of the CIRCIA regulatory program. The information contained in these reports will provide increased visibility into malicious cyber activity, improve our understanding of cross-sector risks, and strengthen our collective defense.

The Federal Government is prioritizing measures to harmonize baseline regulatory requirements across sectors. Chaired by the Federal Communications Commission (FCC), the Cybersecurity Forum for Independent and Executive Branch Regulators enables Federal agencies to coordinate efforts to improve the effectiveness and consistency of regulatory activity. In September 2023, the Cyber Incident Reporting Council delivered a report to Congress on streamlining and harmonizing Federal cyber incident reporting requirements.

★ ★ ★ ★ ★ ★

In July 2023, ONCD invited public responses to a Request for Information on opportunities for, and obstacles to, harmonizing baseline cybersecurity requirements for critical infrastructure and related assessments and audits. Respondents stressed the importance of leveraging existing frameworks and best practices, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), to facilitate reciprocity, and recommended that ONCD work with the federal regulatory agencies to deconflict current and emerging cybersecurity requirements to drive harmonization.

Requirements are most often effective when they align with existing cybersecurity frameworks, voluntary consensus standards, and other technical guidance. In March 2023, CISA updated its Cybersecurity Performance Goals (CPGs) based on stakeholder input and engaged SRMAs to begin to develop sector-specific goals through a phased approach. In February 2024, NIST published version 2.0 of its CSF, which provides updated guidance on managing an evolving cybersecurity risk landscape, implementation, and measuring effectiveness. In the energy sector, the Department of Energy (DOE) partnered with the National Association of Regulatory Utility Commissioners (NARUC) to develop cybersecurity baselines for electric distribution systems and distributed energy resources. In February 2024, NARUC and DOE publicly released the baselines and kicked off phase two to develop implementation strategies and adoption guidelines with state regulatory bodies and industry.

Enhancing Federal Coordination and Partnerships

The Federal Government is modernizing its critical infrastructure protection policies to ensure that Federal cyber capabilities are exercised in a clear, coordinated, and effective manner. In April 2024, the Administration issued NSM-22 on *Critical Infrastructure Security and Resilience*, replacing Presidential Policy Directive 21 (PPD-21) as the Federal Government's primary policy document governing critical infrastructure security and resilience. Released more than 10 years ago, PPD-21 defined 16 critical sectors and assigned responsibility for identifying and managing cyber and other all-hazards risks. NSM-22 strengthens the Federal Government's ability to enable cross-sector cyber defense; clarifies CISA's role as the National Coordinator for the Security and Resilience of Critical Infrastructure; improves connectivity with other Federal agencies serving as SRMAs; and enhances integration and information sharing with law enforcement, the intelligence community, and critical infrastructure owners and operators. NSM-22 also better positions the Federal Government to balance collaboration with regulation, directing SRMAs and sector-specific regulators to develop minimum security requirements. CISA, as the National Coordinator, will engage with SRMAs to develop updated risk assessments and the National Infrastructure Risk Management Plan.

CISA plays a central role in enabling critical infrastructure owners and operators to defend themselves. In 2023, CISA's Joint Cyber Defense Collaborative (JCDC) completed three joint cyber defense plans to enhance the cybersecurity and resilience of critical infrastructure partners. JCDC's remote monitoring and management (RMM) and open-source software (OSS) plans manage cross sector risk by addressing the exploitation of RMM software and producing best practice guidance for the secure use of OSS in operational technology, respectively. JCDC also published an incident response guide for the water and wastewater sector to support small- and

medium-sized utilities. CISA established the Ransomware Vulnerability Warning Pilot (RVMP) program as authorized by CIRCIA to identify commonly exploited vulnerabilities related to ransomware activity, and warn critical infrastructure entities so that they can mitigate the risk. In 2023, this program notified critical infrastructure owners and operators of 1,754 vulnerable devices. And, in November 2023, CISA launched a voluntary pilot program to provide organizations in the healthcare, water and wastewater, and education sectors with cybersecurity shared services.

SRMAs further enable the Federal Government to support and engage with critical infrastructure owners and operators at scale. In 2023, the Department of Health and Human Services (HHS) released a new strategy for healthcare cybersecurity; updated its Health Industry Cybersecurity Practices Guide in collaboration with the Health Sector Coordinating Council; launched the Risk Identification and Site Criticality Tool version 2.0; and partnered with CISA to develop sector-specific CPGs. The Environmental Protection Agency (EPA) released a new cybersecurity risk assessment resource for water and wastewater systems and, in partnership with CISA and the Federal Bureau of Investigation (FBI), developed an incident response guide for the sector. The Treasury Department established the Cloud Executive Steering Group to enhance cooperation between regulators and financial services organizations to address benefits and challenges associated with cloud adoption. DOE, through the Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program, has established new partnerships with key private sector organizations to strengthen the cybersecurity of priority energy system component software, hardware, and firmware.

The Federal Government is focused on supplementing SRMAs' traditional strengths in information sharing and stakeholder engagement with more robust capabilities for operational collaboration with the private sector, including planning, exercises, and incident response. The National Security Agency (NSA) collaborates with private sector partners to defend National Security Systems (NSS), U.S. military assets, and the DIB against cyber threats. The NSA's Cybersecurity Collaboration Center (CCC) provides a scalable, intelligence-driven mechanism for public-private collaboration with the DIB and their service providers, totaling over 750 partnerships in 2023 and further enabling collaborative defense against malicious cyber activity that threatens other critical infrastructure sectors. The CCC continues to expand its cybersecurity support to the DIB, including through providing Protective Domain Name System, Attack Surface Management, and threat intelligence collaboration services.

In response to cyberattacks affecting U.S. school systems, the White House convened a forum to coordinate public and private measures to strengthen the cybersecurity of K-12 schools. The Department of Education established a Government Coordinating Council (GCC) to enhance communication among education subsector stakeholders and improve cybersecurity resilience efforts. The FBI continues to engage with school districts across the country through its 56 field offices to enable on-the-ground cyber threat response services. CISA is providing additional resources to support the education subsector, including developing subsector-specific guidance in partnership with the Department of Education and providing tailored assessments, exercise support, and training to K-12 stakeholders.

★ ★ ★ ★ ★ ★

The National Space Council, the National Security Council Cybersecurity Directorate, and ONCD are also coordinating public and private efforts to address unique challenges related to space system cybersecurity. In 2023, ONCD convened a series of regional technical workshops with government and industry space experts to discuss cybersecurity challenges and opportunities. In July, NIST released an updated report on cyber risk management practices related to commercial satellite operations. In October, the National Aeronautics and Space Administration (NASA) issued a best practices guide to address new challenges by increasingly integrated and interconnected space systems.

State, local, Tribal and territorial (SLTT) governments are working to elevate their cybersecurity posture. The Bipartisan Infrastructure Law provides $1 billion in funding to boost SLTT capacity to address cybersecurity risks to information systems they own or operate. In 2023, CISA and the Federal Emergency Management Agency made available $375 million through the State and Local Cybersecurity Grant Program and $18 million through the Tribal Cybersecurity Grant Program. The Small Business Administration (SBA) also provides grant funding through the SBA Cybersecurity for Small Business Pilot Program. Federal agencies will continue to partner with SLTT entities and small businesses to share cybersecurity best practices, support cyber response and recovery, and accelerate cybersecurity research and development.

Improving Incident Preparedness and Response

The Federal Government continues to prioritize providing support to victims of cyber incidents. The Department of Justice (DOJ), FBI, CISA, U.S. Secret Service, and other Federal entities invest significant resources in helping victims after cyber incidents, including investigating cybercriminals to seek justice and prevent crime; employing a global network of cyber threat experts contributing to attribution and analysis; sharing cyber threat information to inform victim response actions; introducing targeted entities to decryption capabilities or other known mitigation tools; and assisting in freezing, seizing, and returning stolen and extorted funds.

The FBI's Internet Crime Complaint Center Recovery Asset Team streamlines communications with financial institutions and FBI field offices to assist with freezing, seizing, and returning funds for victims and had a 71% success rate in 2023. The FBI-led Cryptocurrency Threat Center has worked with law enforcement and intelligence community partners to increase the U.S. Government's capability to publicly identify stolen cryptocurrency, including virtual assets stolen by DPRK-linked actors. The FBI's Cyber Action Team and a growing number of Model Cyber Squads being developed across all 56 FBI field offices provide a rapid-response capability that can be deployed within hours to provide investigative support in response to a major incident.

CISA Hunt and Incident Response teams support organizations responding to cybersecurity incidents, including by identifying and detecting cyber threats to U.S. critical infrastructure. In 2023, CISA regularly engaged with SRMAs to enhance collaboration with and support to critical infrastructure owners and operators. In addition, the Bipartisan Infrastructure Law established a $100 million Cyber Response and Recovery Fund that CISA can use to support Federal, SLTT, public, and private sector entities in the event of a significant cyber incident.

★ ★ ★ ★ ★ ★

In response to significant incidents and malicious cyber activity, Cybersecurity Advisories (CSA) provide critical infrastructure owners and operators and other entities with timely guidance to detect and respond to threats. Coordinating the development of these CSAs across the Federal Government and with international allies and partners improves support to victims. In May 2023, NSA, CISA, FBI, DOE, and international partners released a CSA detailing the tactics, techniques, and procedures (TTPs) of the PRC-sponsored Volt Typhoon actor, and later provided joint guidance for organizations to identify and mitigate these TTPs.

The Cyber Safety Review Board (CSRB) reviews and assesses significant cyber incidents and makes recommendations for public and private sector organizations to prevent similar incidents from taking place. In August 2023, the CSRB released its analysis of the Lapsus$ threat actor group, highlighting the group's exploitation of systemic ecosystem weaknesses to victimize organizations across the country. This report led to subsequent, ongoing efforts by CISA and DHS to ensure that necessary security features are provided to customers without additional cost. The CSRB's third report, released in April 2024, focuses on the malicious targeting of cloud computing environments and makes recommendations for strengthening identity management and authentication in the cloud. The structured analysis performed by the CSRB plays a crucial role in identifying and sharing lessons learned from significant cyber incidents and developing actionable mitigations.

CISA is committed to updating the National Cyber Incident Response Plan (NCIRP) by the end of 2024. The NCIRP outlines our national approach to handling significant cyber incidents, including defining key roles and responsibilities for Federal agencies, private sector entities, and SLTT entities, in accordance with Presidential Policy Directive 41, *United States Cyber Incident Coordination*. The cyber threat landscape and the cyber defense ecosystem have evolved significantly since the NCIRP was originally published in 2016. The updated NCIRP will provide a modern, agile, flexible framework to enable coordinated national incident response across the Federal Government, private sector, and other key partners.

Disrupting and Degrading Adversary Activity

The United States remains postured to use all instruments of national power to defend our interests in cyberspace and to disrupt and dismantle cyber threat actors. To counter ransomware and other forms of cybercrime, the Administration is pursuing new measures to improve the integrated use of diplomatic, information, military, financial, intelligence, and law enforcement capabilities, and to engage non-Federal and international partners in these activities. Disruption alone cannot defeat ransomware or other forms of malicious cyber activity, but it can have a meaningful impact on the problem.

In September 2023, the DoD finalized its *2023 Department of Defense Cyber Strategy*, which highlights the use of cyberspace operations through its policy of defending forward to actively disrupt malicious cyber activity before it can affect the United States and its interests. In March 2024, DoD released the *Defense Industrial Base Cybersecurity Strategy* to provide an actionable framework for sustaining a more resilient Joint Force and defense ecosystem. In 2023, U.S. Cyber Command's Cyber National Mission Force deployed 22 times to 17 countries to conduct

partner-enabled hunt forward operations that identify malicious cyber activity abroad and constrain adversaries' freedom of maneuver.

In October 2023, the White House-led Counter-Ransomware Initiative (CRI) convened its third summit to coordinate international efforts to defeat ransomware activity around the world. This year, the CRI focused its efforts on developing capabilities to disrupt ransomware attacks and infrastructure, improve information sharing, and fight back against the structural underpinnings of the ransomware ecosystem. To achieve these objectives, the CRI announced new commitments to establish intelligence sharing and operational collaboration platforms, build the cyber capacity of CRI members, and jointly issue the CRI's first-ever policy statement that member governments should not pay ransoms.

When the United States coordinates with allies and partners, takedowns and other disruption activities are more effective, impose more severe consequences on adversaries, and provide more impactful support to victims. These activities can also be paired with diplomatic actions, economic sanctions, and other tools tailored to impact malicious cyber actors. Allies and partners are also making significant contributions to the production of joint CSAs that attribute malicious cyber activity and provide important details on adversary TTPs. To enable additional information sharing and operational collaboration with foreign partners, the FBI has expanded its overseas presence of cyber assistant legal attaches by nearly 40%.

The private sector also plays an important role in enhancing awareness of cyber threats across critical infrastructure through cyber threat intelligence sharing. Private sector organizations often have visibility into certain aspects of malicious activity that the Federal Government does not. The willingness of these organizations to share information directly with law enforcement or through NSA's CCC or CISA's JCDC strengthens the Federal Government's ability to assess and understand threats, devise mitigations, and facilitate victim notifications.

The Federal Government is working to establish rules to prevent malicious actors from abusing U.S.-based cloud, AI, and other third-party services. In January 2024, consistent with EO 14110 on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* and EO 13984 on *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*, the Department of Commerce proposed a rule requiring U.S. Infrastructure-as-a-Service providers to prevent the abuse of their products and services by foreign persons to enable malicious cyber activity.

The Federal Government has increased the speed, scale, and impact of disruption campaigns to counter cybercriminal activity and dissuade adversaries from using cyber capabilities to achieve their malicious goals. The following campaigns illustrate the range of recent U.S. actions to disrupt malicious cyber activity affecting victims around the world:

- **January 2023**: DOJ announced a disruption campaign against the HIVE ransomware group, which had claimed over 1,500 victims in over 80 countries. The FBI and international partners penetrated HIVE networks, took its decryption keys, and made those keys available to victims. CISA, the FBI, and HHS disseminated HIVE indicators of compromise (IOCs) and TTPs through a joint CSA.

★ ★ ★ ★ ★ ★

- **May 2023**: DOJ announced an operation code-named MEDUSA which disrupted a sophisticated global malware network called Snake. The operation disabled the malware on compromised computers using a tool created by the FBI. Simultaneously, the FBI, NSA, CISA, DoD Cyber National Mission Force, and international partners released a joint CSA attributing the malware to Russia's Federal Security Service (FSB).

- **July 2023**: CISA announced the prevention of over 400 attempted ransomware operations since the beginning of the year. CISA disrupted these operations by passing to victims technical information paired with advice on how to best prevent further exploitation or harm.

- **August 2023**: DOJ announced a multinational operation which disrupted the Qakbot botnet and malware and took down its infrastructure. In 2023, cybercriminals used this infrastructure to commit ransomware, financial fraud, and other forms of criminal activity around the world. Dismantling this botnet involved gaining comprehensive access to compromised infrastructure and deploying a custom script to remove the malicious code from victim computers. FBI also seized $8.6M in cryptocurrency in illicit profits. CISA and the FBI disseminated Qakbot infrastructure IOCs through a joint CSA.

- **December 2023**: DOJ announced a disruption campaign against the ALPHV/Blackcat ransomware group, which had claimed over 1,000 victims around the world. At the time, ALPHV/Blackcat was the world's second-most popular ransomware-as-a-service variant, presenting would-be cybercriminals with an easy-to-use toolset for executing extortion ransomware attacks. The FBI developed a decryption tool that enabled field offices and international partners to provide support to affected victims. CISA and the FBI disseminated ALPHV/Blackcat IOCs and TTPs through a joint CSA.

- **December 2023**: DOJ announced that Anatoly Legkodymov, the founder and majority owner of Bitzlato Ltd., a cryptocurrency exchange that served as a primary conduit for dark market purchasers and sellers, as well as a safe haven for illicit transactions by ransomware criminals, pleaded guilty to operating a money transmitting business that transmitted illicit funds.

- **January 2024**: DOJ announced a court-authorized online operation that disrupted a botnet that PRC state-sponsored actors used to conceal the hacking of U.S. and allied critical infrastructure. The PRC actors used a botnet comprised of small home/small office (SOHO) routers to obfuscate their hacking of, and enduring surreptitious access to, U.S. critical infrastructure networks. FBI, CISA, and NSA issued several CSAs with detailed technical information about the PRC TTPs, allowing cybersecurity professionals to detect and prevent similar intrusions into their networks.

- **February 2024:** DOJ announced a disruption campaign, in coordination with other international law enforcement partners, of the LockBit ransomware group, which had claimed over 2,000 victims around the world. The United Kingdom, in cooperation with the FBI and other partners, also developed decryption capabilities for affected victims.

★ ★ ★ ★ ★ ★

- **February 2024**: DOJ announced an online operation to disrupt a botnet comprised of thousands of compromised SOHO routers operated by Russia's military intelligence agency, the GRU. The GRU created this botnet by co-opting criminal hackers' earlier compromise of SOHO routers with Moobot malware and turning them into a global intelligence collection platform, primarily in support of spearphishing and similar credential harvesting campaigns, including operations targeting Ukraine. This takedown was the third time since Russia's invasion of Ukraine that the United States stripped the Russian intelligence services of a key tool used to further Russia's acts of aggression and other malicious activities.

Defending Federal Networks

In response to significant cyber incidents targeting Federal networks and critical infrastructure, EO 14028 marked a paradigm shift in the Federal Government's approach to cybersecurity by establishing baseline security measures across Federal systems. NSM-8 further transformed accountability for the cybersecurity of our nation's most critical systems by clarifying responsibilities for securing NSS. In addition, the Administration crafted a cybersecurity modernization agenda to invest in systems that support collective defense and created the first strategy to adopt Zero Trust Architecture (ZTA) across the Federal civilian enterprise.

In 2023, Chief Financial Officer (CFO) Act civilian agencies made progress implementing high-impact cybersecurity practices to improve their cybersecurity posture. These practices include progress on encrypting data both in transit and at rest, deployment of phishing-resistant multi-factor authentication (MFA), deployment of end-point detection and response (EDR) services, logging capabilities, and hiring skilled cybersecurity teams. By the first quarter of fiscal year 2024, CFO Act civilian agencies demonstrated the following achievements as measured by quarterly Federal Information System Modernization Act metrics:

- **Encryption:** Progress was reported in encryption of data both at rest and in transit, with multiple CFO Act civilian agencies showing increases of more than 10%.

- **MFA:** There were improvements in the deployment of phishing-resistant MFA across the vast majority of agencies, with ten agencies demonstrating an increase of at least 20% phishing-resistant MFA deployment on agency systems.

- **EDR:** The average percentage of endpoints covered by at least one EDR platform reached 92%.

- **Logging:** Five agencies achieved "advanced" logging capabilities for all High Value Assets. The Office of Management and Budget (OMB) and CISA stood up a working group to drive more effective log collection, which supports incident response activities.

- **Skilled Cybersecurity Team Hiring:** Agencies continued to strengthen skilled cybersecurity team hiring, achieving an average position fill rate of 91%.

★ ★ ★ ★ ★ ★

Defending Federal systems at speed and scale requires the government to advance an enterprise-level view of risk across departments and agencies. Through the adoption of shared services, agencies have bolstered their capabilities, reduced their attack surfaces, and improved visibility across Federal networks. In October 2023, OMB and ONCD convened an interagency working group that explored the deployment and use of cybersecurity shared services across the Federal Government, interviewed providers and customers, and identified gaps and challenges in getting shared services to small and micro agencies.

CISA has equipped agencies with greater capabilities to identify, prioritize, and mitigate cybersecurity risks while enabling them to understand and manage critical threats through its Continuous Diagnostics and Mitigation (CDM) program, which is aligned to government-wide documents such as the Known Exploited Vulnerabilities catalog. In 2023, CISA helped enable the shift toward shared services by expanding its CDM program to all 23 civilian CFO Act agencies and 69 non-CFO Act agencies, and by onboarding 97 agencies onto their Protective Domain Name System service.

CISA, OMB, and ONCD have engaged with industry to determine the feasibility of providing enhanced logging capabilities to Federal civilian executive branch agencies. In February 2024, these engagements resulted in the rollout of expanded logs to all agencies and the extension of the default log retention period from 90 to 180 days. This major step forward is in line with CISA's Secure by Design guidance, which calls for technology providers to furnish "high-quality audit logs to customers at no extra charge."

The Director of NSA, as the National Manager for NSS, continues to enhance cyber coordination and alignment across over 70 Federal departments and agencies through greater centralized accountability, alignment of policy processes, and formalization of standards for NSS across Federal owners and operators.

ONCD, in collaboration with interagency partners, developed a plan to drive improvements in Internet routing security, focusing on addressing vulnerabilities in the BGP. These vulnerabilities can be addressed by solutions such as Resource Public Key Infrastructure Route Origin Authorizations (RPKI ROA). The Federal Government has developed a Legacy Registration Services Agreement template for Federal agency use, and is developing a playbook to facilitate adoption of RPKI ROA. This solution removes a significant barrier to adoption and will facilitate government-wide implementation of RPKI ROA.

Efforts are also underway to improve collective operational defense so that breaches are isolated and remediated rapidly. CISA's Persistent Access Capability, made possible through the widely adopted EDR initiative born out of Executive Order 14028, facilitates real-time threat intelligence sharing. The Federal Government's deliberate shift toward ZTA, the expansion of shared services, and the maturation of collective operational defense reflects a concerted effort to address the current cyber threat landscape and prepare for future challenges.

★ ★ ★ ★ ★ ★

Strengthening the National Cyber Workforce

The number of unfilled cyber jobs nationwide presents both a national security challenge and a tremendous economic opportunity, with public and private sector organizations pursuing a wide range of creative solutions. Released in July 2023, the National Cyber Workforce and Education Strategy (NCWES) prioritizes whole-of-government and whole-of-society approaches to address the immediate needs of the cyber workforce. The NCWES focuses on three guiding imperatives: (1) leverage collaborative workforce development ecosystems to meet cyber workforce demands; (2) enable the lifelong pursuit of cyber skills; and (3) strengthen the cyber workforce through greater diversity and inclusion.

Senior officials from across the Federal Government conducted strategic outreach engagements across the United States to gather perspectives from workers, educators, employers, and government leaders at local, state and Federal levels on cyber workforce matters. As of March 2024, more than 90 organizations had made commitments in support of the NCWES, including hiring over 13,000 people in cyber jobs, dedicating over $280 million toward equipping Americans with foundational cyber skills, transforming cyber education, expanding the national cyber workforce, and strengthening the Federal cyber workforce.

The NCWES makes clear that access to cyber education is necessary to meet our national cyber workforce needs in a sustainable manner. More than 440 colleges and universities designated by NSA as National Centers of Academic Excellence in Cybersecurity (NCAE-C) deliver rigorous cybersecurity education to thousands of students each year. More than 100 of these NCAE-C institutions participate in the CyberCorps®: Scholarship for Service (SFS) program led by the National Science Foundation (NSF) in collaboration with DHS and OPM. To prepare students in high school to enter these programs, Career and Technical Education (CTE) programs funded by the Department of Education are expanding their reach into middle schools with technical skill development as well as career advising and navigation. The GenCyber program, administered by NSA and funded through NSA and NSF, is developing the cyber skills of K-12 teachers and students in informal summer camp learning environments. With consistent and dedicated Federal support, these efforts can continue to expand innovation in STEM education and provide a foundation for sustained development of the national cyber workforce.

The NIST NICE program coordinates Federal Government cybersecurity education and workforce programs through the NICE Interagency Coordinating Council. NICE also promotes and energizes a community working together through the NICE Community Coordinating Council which includes working groups that implement the NICE Strategic Plan. NICE supports the ongoing development of CyberSeek.org which provides an interactive jobs heat map and a cooperative agreement for the U.S. Cyber Games resulting in the annual selection of the U.S. Cyber Team. Updated in March 2024, the NICE Workforce Framework for Cybersecurity establishes a common lexicon that describes cybersecurity work and workers for the public and private sectors.

Cyber workforce and education efforts are most effective when they align skill development—beginning in elementary school with career awareness, through career navigation in the middle

grades, and technical skill preparation in high school—with progression into employment, higher education, entrepreneurship, or enlistment in the military. Examples of these programs include:

- Through the CHIPS and Science Act, NSF's Regional Innovation Engines program provides planning grants to grow Cyber Workforce ecosystems. In May 2023, NSF announced 44 Engines Development Awards spanning 46 U.S. states and territories, each funded at up to $1 million over two years to plan for a future NSF Engine.

- The annual NICE K-12 Cybersecurity Education Conference and NICE K-12 Community of Interest support the professional development of teachers and provide school administrators with the strategies and resources necessary to promote the discovery of cybersecurity careers.

- In April 2023, NIST awarded cooperative agreements to 18 Regional Alliances and Multistakeholder Partnerships Stimulating (RAMPS) cybersecurity education and workforce development program recipients in 15 different states, and in March 2023 introduced a Notice of Funding Opportunity for 15 additional awards. These RAMPS Communities created an integrated ecosystem of cybersecurity education and workforce development to support local and regional economies.

- The Department of Education provides Career and Technical Education formula grants to states that can be used for cybersecurity skills development.

- The General Services Administration (GSA) operates the cross-government U.S. Digital Corps (USDC) fellowship program. In 2023, USDC recruited 47 early career technology talents to the Federal Government, including nine Cybersecurity Fellows.

- DOE has multiple cyber workforce and education programs targeting the energy sector. CyberForce is a collegiate cyber defense competition to test skills in team and individual competitions. The Operational Technology (OT) Defender Fellowship gives middle- and senior-level OT security managers in the energy sector the opportunity to learn about the strategies used to target energy infrastructure and the cybersecurity tools and tactics used to counter them. CyberStrike is a hands-on ICS-focused training that supports pipeline and re-skilling workforce development efforts for energy sector owners and operators.

- In March 2024, DOE announced $15 million in funding to establish six university-based electric power cybersecurity centers that will foster collaboration across the energy sector to address gaps in energy security research and provide cybersecurity education.

Departments and agencies are also crafting workforce development approaches that meet their specific needs, recognizing that a diverse and varied set of pathways can provide the skills needed in the cyber workforce. For example, DoD released the *DoD Cyber Workforce Strategy 2023-2027* and accompanying implementation plan to address how the Department will foster a skilled and diverse cyber workforce. OPM has developed a legislative proposal addressing government-wide challenges and opportunities to strengthen and better compensate the Federal cyber workforce.

★ ★ ★ ★ ★ ★

Advancing Software Security to Produce Safer Products and Services

Improving software security will reduce systemic risk across the digital ecosystem. To seize this opportunity, the Federal Government has engaged with industry, academia, and civil society to promote Secure by Design principles and practices that shift the responsibility for security onto those organizations that are best positioned and most well-resourced to mitigate risk. These actions lay the groundwork for possible legislation to establish liability for cybersecurity vulnerabilities in software products and services.

In April 2023, CISA released *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design*, a guidance document developed with U.S. and international partners to provide organizations with concrete steps to implement Secure by Design principles. In October 2023, CISA and its partners, including eight new international agency co-sealers, published an update to the joint guidance to reflect feedback from hundreds of stakeholders. At the end of 2023, CISA also released its first Secure by Design alerts to provide guidance on secure software development practices and security defenses in technology products.

In March 2024, CISA released the Secure Software Development Attestation Form, which will help ensure that the software producers who sell to the Federal Government leverage secure development techniques and toolsets. The form was drafted in consultation with OMB and based on practices established in the NIST *Secure Software Development Framework*.

Software Bills of Material (SBOM) can enhance software supply chain risk management practices. In December 2023, NSA, ODNI, and CISA released a technical report containing guidance for industry on effective implementation of SBOM and the safe integration of open-source components into the software development lifecycle. That same month, NSA released *Recommendations for Software Bills of Materials (SBOM) Management*, which highlights best practices and provides recommendations for NSS to incorporate SBOM management functions suitable to their cybersecurity supply chain risk management needs.

The adoption of memory safe programming languages enables the software development ecosystem to produce safer products and services. Memory safe programming languages can benefit both open-source and proprietary software and eliminate entire classes of vulnerabilities across the digital ecosystem. In December 2023, technical experts from CISA, NSA, FBI, and international partners released *The Case for Memory Safe Roadmaps*, containing practical guidance for organizations seeking to adopt memory safe programming languages in their environments. In February 2024, ONCD released *Back to the Building Blocks: A Path Toward Secure and Measurable Software* to highlight memory safety and software measurability as two security challenges that the technical community can help solve.

The Federal Government has made it a priority to support the open-source developer community and enable the secure integration of open-source components. The Open-Source Software Security Initiative (OS3I) convenes public and private sector stakeholders to increase the security and resilience of the open-source software landscape. In August 2023, ONCD sought public input on open-source software security and memory safe programming languages. CISA also released an *Open-Source Software Security Roadmap* to prioritize its work in this space.

★ ★ ★ ★ ★ ★

Enabling a Digital Economy that Empowers and Protects Consumers

The American public must be able to participate in a digital economy that is safe, fair, and accessible, and produces hardware and software that are reliably secure against cyber threats. The Administration has pursued a range of market shaping tools to empower consumers, promote innovation, and incentivize cyber-secure competition.

In March 2024, the FCC approved the *U.S. Cyber Trust Mark*, a voluntary cybersecurity certification and labeling program that will help Americans purchase smart devices that are safer and less vulnerable to cyberattacks. Under the program, IoT devices that meet certain cybersecurity criteria as determined by NIST, such as requiring unique and strong default passwords or securely implementing software updates, will be eligible for certification. Already, several leading consumer electronics manufacturers and retailers have committed to supporting implementation of the program. In July 2023, DOE announced a labeling research effort to address the feasibility and limitations of applying a labeling approach to OT like smart meters and solar inverters.

The Administration has taken steps to ensure that Federal spending increases our collective cybersecurity and resilience. DoD, the General Services Administration (GSA), and NASA have proposed amendments to the Federal Acquisition Regulation (FAR) to standardize and improve cybersecurity requirements for unclassified Federal information systems, including prohibiting agencies from buying vulnerable IoT devices and requiring the use of SBOMs. Raising the cybersecurity standards of Federally-procured technology products will incentivize cybersecurity across the ecosystem.

Under the False Claims Act, the DOJ's Civil Cyber-Fraud Initiative holds government contractors accountable when they materially misrepresent the cybersecurity attributes of their products or services. In 2023, DOJ reached settlements with two vendors who had misrepresented that their products met cybersecurity controls tied to Federal contracts.

At the end of 2023, the Treasury Department completed its initial assessment of the need for a Federal insurance response to catastrophic cyber events, finding that further exploration of the appropriate form of such a response is warranted and would be undertaken in the next phase of the assessment, in coordination with CISA and ONCD. CISA also announced the reconstitution of the Cybersecurity Insurance and Data Analysis Working Group to create a venue for government and industry stakeholders to exchange information and discuss the role of the insurance industry in driving down cyber risk.

Investing in Resilient Next-Generation Technologies

Embedding security and resilience into the technological foundations of our digital ecosystem is a cheaper and more efficient approach than attempting to bolt it on after the fact. In 2023, American innovation and public investment, powered by the President's Invest in America Agenda, created opportunities for coordinated public-private efforts to optimize critical and emerging technologies for cybersecurity as they are developed and deployed. For example, in November 2023, DOE announced $70 million in funding through the Rural and Municipal

★ ★ ★ ★ ★ ★

Utility Advances Cybersecurity Grant and Technical Assistance BIL Program to enhance the cybersecurity posture of electric cooperative, municipal, and small investor-owned utilities. This program helps these smaller utilities protect against, detect, respond to, and recover from cybersecurity threats, and increases their participation in cybersecurity threat information sharing programs.

The ongoing clean energy transition presents opportunities to build in security and resilience across the foundations of our national infrastructure and clean energy supply chains. Through implementation of grant programs included in the BIL and IRA, DOE and other Federal partners are enabling grant recipients to procure and implement safer clean energy technologies. The BIL also requires that certain projects funded under the law include a cybersecurity plan to maintain or improve the project's cybersecurity over its lifecycle.

In July 2023, DOE funded eight innovative small businesses that are advancing cybersecurity for distributed energy resources (DERs) and in September announced $39 million of funding for nine new National Laboratory projects to advance the cybersecurity of DERs. Also in September 2023, the DOE Clean Energy Cybersecurity Accelerator graduated its inaugural cohort, focusing on enabling technologies that offer authentication and authorization solutions for industrial control systems. DOE further released an implementation guide for its National Cyber-Informed Engineering Strategy to assist organizations in building cybersecurity into the design of energy infrastructure. In January 2024, DOE also announced a $30 million funding opportunity to support research, development, and demonstration (RD&D) of next generation tools to protect clean energy delivery infrastructure from cyberattacks.

The Federal Government is funding RD&D in cutting-edge cybersecurity and resilience technologies. The *2023 Federal Cybersecurity Research and Development Strategic Plan* aligns to the NCS and provides Federal agencies with specific guidance on priorities for Federal funding, including human-centered cybersecurity, trustworthiness, cyber resilience, metrics, and RD&D infrastructure. The plan also aligns with an August 2023 joint OMB-OSTP memo outlining multi-agency research and development priorities for the fiscal year 2025 budget, including critical and emerging technology and innovation that can mitigate cybersecurity risk. Through its Secure and Trustworthy Cyberspace program, the NSF is funding research projects focusing on critical infrastructure security and resilience.

The Administration is coordinating public and private actions to secure longstanding vulnerabilities in the underlying technical foundations of the Internet. Making the BGP more secure can significantly reduce harm resulting from unsecured Internet routing. In July 2023, the FCC and CISA convened Federal partners, nonprofits, and industry partners, including Internet service providers and cloud content providers, to develop a common understanding of the latest BGP security improvements and coordinate efforts to accelerate them.

In October 2023, the President signed EO 14110 on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* to direct whole-of-government efforts to shape the values-aligned development of AI. EO 14110 addresses the various ways by which AI may impact the cybersecurity community. First, to explore ways to use AI to enable more efficient cyber defense activities, EO 14110 establishes an advanced cybersecurity program to develop AI

tools to find and fix vulnerabilities in critical software. Second, to mitigate the potential risks posed by AI to our critical infrastructure, EO 14110 directs DHS to establish an AI Safety and Security Board and, based on NIST's AI Risk Management Framework, provide safety and security guidelines to critical infrastructure owners and operators. Third, to protect the AI ecosystem against cyber threats, developers of certain AI models will be required to report to the Department of Commerce their capabilities for defending against sophisticated threat actors.

The Federal Government continues to engage with a wide range of stakeholders to prepare for a post-quantum future. In August 2023, NIST submitted for public comment three draft Federal Information Processing Standards (FIPS) designed to resist future attacks by cryptanalytically-relevant quantum computers. To support non-Federal cryptographic transitions, OMB, CISA, NIST, and NSA published resources for organizations to develop and implement their own Quantum-Readiness Roadmaps. NIST, NSA, and partners are working across multiple standards developing organizations to integrate the expected NIST post-quantum cryptographic standard in a wide variety of security standards. NIST also continues to engage with a working group of industry, academic, and government stakeholders to identify and address the challenges related to cryptographic transitions at the NIST National Cybersecurity Center of Excellence.

Managing Risks to Data Security and Privacy

In the absence of a national data privacy law, the Administration is pursuing targeted measures to protect Americans' data and their privacy, and enable safe, data-rich cross-border commerce. EO 14117 on *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* authorizes the Attorney General to prevent the large-scale transfer of Americans' personal data to countries of concern and provides safeguards around other activities that can give those countries access to Americans' sensitive data. The protections authorized by EO 14117 will extend to genomic data, biometric data, personal health data, geolocation data, financial data, and certain kinds of personal identifiers that adversaries may exploit for a variety of nefarious purposes, including to engage in malicious cyber-enabled activities.

The EU-U.S. Data Privacy Framework, finalized in July 2023, is a leading example of the international partnership required for safe and trusted cross-border data flows. Alongside the framework's finalization, the Department of Commerce released the Data Privacy Framework program website for companies participating in cross-border data transfers.

EO 14110 on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, reinforces the importance of mitigating privacy risks in emerging technologies. EO 14110 directs departments and agencies to take steps to safeguard Americans' privacy in the development and deployment of AI. In December 2023, NIST issued draft guidance for agencies on evaluating differential-privacy-guarantee protections. In February 2024, DOE and NSF established a Research Coordination Network to advance research, development, and implementation of privacy-enhancing technologies (PETs).

PETs are an important part of the Administration's affirmative vision for a secure, trustworthy, and rights-respecting digital ecosystem. To coordinate Federal efforts to harness PETs, the

★ ★ ★ ★ ★ ★

Administration released the *National Strategy to Advance Privacy-Preserving Data Sharing and Analytics* in March 2023. The strategy provides a roadmap for research, development, and adoption of PETs in a manner that will help tackle shared challenges such as healthcare, climate change, financial crime, human trafficking, and pandemic response. The United States has also engaged with international partners and academia stakeholders through the PETs Prize Challenge, which announced winners at the Summit for Democracy in March 2023.

Enhancing Security and Resilience Across the Globe

Cyberspace is a global domain, and the United States works hand-in-hand with allies and partners to defend against common cyber threats and build shared resilience. This approach to collective defense is rooted in both increasingly integrated operational capabilities and deepening strategic alignment. Over the past year, Federal departments and agencies signed new arrangements to strengthen bilateral cooperation with a wide range of foreign partners, including Finland, the Republic of Korea, and Jordan.

Throughout 2023, the United States responded to our partners and allies in times of crisis, supporting countries such as Costa Rica and Albania with funding, resources, and technical expertise to help them recover from cyberattacks. Recent incidents have shown the need for both immediate incident response resources and longer-term technical support to develop more secure and resilient cyber ecosystems.

The Administration continues to expand flexible and innovative pathways for building partner cyber capacity. A new Cyberspace, Digital Connectivity, and Related Technologies Fund, established with support from Congress, recognizes the need for sustained funding mechanisms able to scale to meet our partners' needs in and out of conflict. This instrument, once fully funded, enables the State Department to provide foreign assistance through flexible, robust, and responsive cyber, digital, and emerging technology programs that can be delivered quickly in order to respond to fast moving threats and opportunities.

The Administration also collaborates with allies, partners, and the private sector to build cyber capacity. For example, in December 2023, the Tallinn Mechanism was officially formalized between the United States, Ukraine, and nine other partners as a means to coordinate and facilitate civilian cyber capacity building in support of Ukraine. The Tallinn Mechanism systematizes the assistance and contributions from both governments and the private sector to reinforce Ukraine's long-term cyber resilience and preparedness.

The United States has used regional coalitions—such as the Organization of American States (OAS), Economic Community of West Africa States (ECOWAS), and Association of Southeast Asian Nations (ASEAN)— to build cybersecurity capacity as the demand for cybersecurity assistance grows in both scope and scale. In September 2023, DHS hosted the first Western Hemisphere Cyber Conference, which convened cyber leaders from 21 foreign governments to discuss cybersecurity challenges and identify areas of collaboration. To support global, multistakeholder efforts on sustainable cyber capacity building, the U.S. endorsed the *Accra Call for Cyber Resilient Development: An Action Framework*.

★ ★ ★ ★ ★ ★

In May 2024, the State Department released the *International Cyberspace and Digital Policy Strategy* to lay out the Administration's affirmative vision for digital solidarity, multilateral engagement, coalition building, and strengthening international cyber capacity. A key element of this strategy is working with allies and partners to secure the digital ecosystem so that technologies being designed and deployed today are secure against the threats of tomorrow.

The Administration is prioritizing research and development, standards development, and supply chain security and diversification for technologies such as 5G and 6G, cloud infrastructure and data centers, semiconductors, undersea cables, and satellite communications. The State Department's International Technology Security and Innovation (ITSI) Fund provides $100 million per year over five years to diversify the global semiconductor supply chain, promote secure ICT connectivity, provide agile response programs, and protect Americans' sensitive data from foreign adversaries. The State Department is also strengthening its own expertise and capacity domestically and overseas with expanded training programs and will field a trained cyber-digital policy officer at every mission engaging on these issues by the end of 2024.

Advancing a Rights-Respecting Digital Ecosystem

The United States is working with like-minded allies and partners to ensure that the digital world reflects and reinforces our shared democratic values. Countries around the world are seeking to advance an affirmative, human rights-respecting vision of technology's benefits, while simultaneously working to counter the misuse of technology and the rise of digital authoritarianism.

To meet this challenge, the 2023 and 2024 Summits for Democracy highlighted the commitment of the United States and over 70 countries to advancing an affirmative vision of an open, free, global, interoperable, reliable, accessible, and secure Internet; combatting the proliferation and misuse of digital technologies like commercial spyware; and shaping emerging technologies to align with democratic values and human rights. Many of those countries work alongside the United States to support Internet freedom and protect human rights worldwide through the Freedom Online Coalition. In 2023, the United States assumed the chair of the Freedom Online Coalition and strengthened the coalition's work to shape the standards and norms that underpin Internet freedom.

CISA launched the High Risk Community Protection Initiative to partner with communities who are at heightened risk of advanced persistent threat targeting and have limited capacity to provide for their own defense. CISA has partnered with civil society organizations and technology companies to develop resources which advance the cybersecurity of civil society. Through the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression, CISA has worked with stakeholders in the United Kingdom, Australia, Canada, Denmark, Estonia, France, Japan, New Zealand, and Norway to advance global efforts to strengthen the cybersecurity of civil society and improve its resilience to transnational repression.

The Administration has mobilized a government-wide effort to counter the proliferation and misuse of commercial spyware, one of the most intrusive forms of digital repression. Issued in

March 2023, EO 14093 on *Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security* restricts the U.S. Government's operational use of commercial spyware that poses risks to national security or poses significant risks of improper use by a foreign government or foreign person. EO 14093 was the first step in a broader campaign to counter the threat posed by the proliferation and misuse of commercial spyware, including through: (1) diplomatic engagement, primarily through a coalition of 17 like-minded partners endorsing the U.S.-led *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware* and the *Guiding Principles on Government Use of Surveillance Technologies*; (2) continued use of Department of Commerce export controls on specific commercial spyware vendors; (3) a new State Department visa ban policy targeting those who misuse commercial spyware or benefit from its misuse; and (4) Treasury Department sanctions against commercial spyware vendors and their leadership.

The Administration seeks not only to mitigate the harms of existing vulnerabilities in our digital ecosystem, but also to promote our values through international cyber norms. The United States is committed to promoting the United Nations (UN) framework for responsible state behavior in cyberspace, making progress on confidence building measures, and upholding norms through the UN Open-Ended Working Group. The United States also continues to promote the establishment of the permanent UN Cyber Programme of Action (POA) to advance the UN framework, with 161 governments voting to support the creation of such a mechanism in the General Assembly.

The United States will continue to work with allies, partners, and organizations such as the U.S-EU Trade and Technology Council and International Telecommunication Union to shape technology standards in alignment with U.S. values. In May 2023, the Administration also published the first ever National Standards Strategy for Critical and Emerging Technology which puts forward an affirmative vision of standards that embrace transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and broad participation.

★ ★ ★ ★ ★ ★

Future Outlook

The *2024 Report on the Cybersecurity Posture of the United States* highlights the breadth and depth of cybersecurity initiatives taking place across the Federal Government to realize the NCS's vision of a digital ecosystem that is defensible, resilient, and aligned with our values. While the strategic environment will continue to evolve, presenting new technological and governance challenges as well as opportunities, many of the current programs will continue to endure over the coming years. Each step taken toward the Administration's affirmative vision will strengthen our cybersecurity posture and build economic prosperity for communities across the country.

Along with continued implementation of the Federal Government's current efforts, there are several efforts that will require a specific focus in the coming year. Each of these have resources aligned to them in the fiscal year 2025 President's Budget request.

- Federal agencies with designated responsibilities as an SRMA must continue to enhance their efforts, consistent with U.S. critical infrastructure security and resilience policy and the Homeland Security Act, to enable operational collaboration within their sectors and provide specialized expertise to critical infrastructure owners and operators.

- Departments and agencies will continue to implement the NCWES at scale through a diverse array of programs and authorities to strengthen the national cyber workforce, improve cyber education, and address unique challenges facing the Federal cyber workforce.

- Implementation of CIRCIA will establish new requirements for covered entities across all critical infrastructure sectors to report certain cybersecurity incidents to the Federal Government. The information contained in these reports will provide new visibility into malicious cyber activity and ransomware, improve our understanding of cross-sectoral risks, and strengthen our collective defense. CISA and other departments and agencies with CIRCIA responsibilities are preparing to receive, process, share, and respond to these new incident reports.

- In 2023, DOJ established a new National Security Cyber Section to increase the Department's capacity to disrupt and respond to malicious cyber activity. The Section will promote Department-wide, intragovernmental, foreign, and private sector partnerships to tackle increasingly sophisticated and aggressive cyber threats by nation-state adversaries and their proxies.

- To create a common operating landscape for cybersecurity, CISA is developing a new Cyber Analytics and Data System. This infrastructure will be used to integrate cybersecurity data sets; provide internal tools and capabilities to facilitate the ingestion and integration of data; and orchestrate and automate the analysis of data to support the rapid identification, detection, mitigation, and prevention of malicious cyber activity.

★ ★ ★ ★ ★ ★

- The Federal Government continues to plan the transition of vulnerable public networks and systems to quantum-resistant cryptography, consistent with NSM-10 on *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. In 2023, Federal departments and agencies undertook the first inventory of Federal cryptographic systems which may contain vulnerable encryption algorithms and developed cost estimates for quantum-resistant cryptography migration. These inventories and cost estimates will inform future planning for migration activities.

NCSIP Version 2 builds on the successes of 2023 and creates a blueprint for resource alignment. ONCD is committed to maintaining the transparency of the implementation process and ensuring Federal coherence, and the NCSIP will continue be updated annually to reflect work completed and identify measures required to meet the new demands of the dynamic cyber threat landscape.