INSTITUTE FOR DEFENSE ANALYSES

Summary of National Cybersecurity Strategy with Similarity Analysis to Executive Order 14028, “Improving the Nation’s Cybersecurity”

Kevin Garrison, Project Leader
Pranay N. Bhandare
Travis L. DePriest
Katharina M. Gallmeier
Arun S. Maiya

March 2023

Approved for public release;
distribution is unlimited.

IDA Non-Standard D-33439

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

About This Publication

This work was conducted by the IDA Systems and Analyses Center under Project C5107, “Cyberspace Operations Working Group,” for IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or any other sponsoring organization.

Acknowledgements

Priscilla E. Guthrie (ITSD)

For More Information

Kevin Garrison, Project Leader
kgarriso@ida.org, 703-933-6545

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

Executive Summary

The National Cybersecurity Strategy was released in early March 2023. As described in the President's cover letter, the strategy "details the comprehensive approach my Administration is taking to better secure cyberspace and ensure the United States is in the strongest possible position to realize all the benefits and potential of our digital future."

The introduction addresses the strategic environment by discussing emerging trends and naming malicious actors. It outlines the overall approach of rebalancing the responsibility for defending cyberspace and realigning incentives to favor long-term investments. Finally, it discusses how the strategy builds on existing policy and replaces the 2018 National Cyber Strategy.

The body of the documents addresses five pillars, with supporting strategic objectives:

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

This document is a reformatted and slightly abridged version of the National Cybersecurity Strategy that also includes some analytical products developed using IDA's internal natural language processing tools. The products include word clouds, showing the most commonly used significant terms in the strategy, thematic clouds highlighting key terms for some of the pillars, and, finally, a similarity analysis comparing the strategic objectives in the strategy to the sections in Executive Order 14028, *Improving the Nation's Cybersecurity*, which was released May 12, 2021.

National Cybersecurity Strategy – March 2023[1]

POTUS

- Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense.
- This strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace.
- We must ensure the Internet remains open, free, global, interoperable, reliable, and secure—anchored in universal values that respect human rights and fundamental freedoms.

Introduction

- The Internet has transformed our world.
- The digital ecosystem reflects the values of its architects and users.
- We have grand ambitions for the further values-driven development of our digital ecosystem.
  - Building a smart grid
  - Maturing Internet of Things (IoT)
  - Laying foundations for real-time global collaborations leveraging vast amounts of data and computing power.
- Achieving vision depends on cybersecurity and resilience of underlying technologies and systems.
- Must make fundamental changes to underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it.
- This strategy will position the United States and its allies and partners to build that digital ecosystem together, making it more easily and inherently defensible, resilient, and aligned with our values.

Strategic Environment

Emerging Trends

- The world is entering a new phase of deepening digital dependencies.
- Software and software systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity.
- The Internet continues to connect individuals, businesses, communities, and countries on shared platforms that enable scaled business solutions and international exchange. But this accelerated interconnectivity also introduces risks.
- Digital technologies increasingly touch the most sensitive aspects of our lives, providing convenience, but also creating new, often unforeseen risks.
- Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing some of our most essential systems to disruption.
- Increasing use of digital operational technology (OT).

Malicious Actors

- Malicious cyber activity has evolved from nuisance defacement, to espionage and intellectual property theft, to damaging attacks against critical infrastructure, to ransomware attacks and influence campaigns designed to undermine public trust in the foundation of our democracy.
- Governments of China, Russia, Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms.
- The People's Republic of China (PRC) now presents the broadest, most active, and most persistent threat to both government and private sector networks and is the only country with both the international order and, increasingly, the economic, diplomatic, military, and technological power to do so.
- For more than two decades, the Russian government has used its cyber capabilities to destabilize its neighbors and interfere in the domestic politics of democracies around the world.
- The governments of Iran and the Democratic People's Republic of Korea (DPRK) are similarly growing in their sophistication and willingness to conduct malicious activity in cyberspace.
- The cyber operations of criminal syndicates now represent a threat to the national security, public safety, and economic prosperity of the United States and its allies and partners.

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Approach

Pillars +"Two Fundamental Shifts"

- Deep and enduring collaboration between stakeholders across our digital ecosystem will be the foundation upon which we make it more inherently defensible, resilient, and aligned with U.S. values.
- Each pillar requires unprecedented levels of collaboration across its respective stakeholder communities, including the public sector, private industry, civil society, and international allies and partners.
- The pillars organizing this strategy:
  - Articulate a vision of shared purpose and priorities for these communities
  - Highlight challenges they face in achieving the vision
  - Identify strategic objectives around which to organize their efforts.
- Two fundamental shifts in how the United States allocates its roles, responsibilities, and resources in cyberspace.

Shift #1: Rebalance the Responsibility to Defend Cyberspace

- The most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem.
  - End-users bear too great a burden for mitigating cyber risks.
  - Have limited resources and competing priorities.
  - Individual choices can impact national security.
- Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens.
- Must ask more of the most capable and best-positioned actors to make our digital ecosystem secure and reliant.
- Protecting data and assuring reliability of critical systems must be the responsibility of owners and operators of the systems that hold our data and make our society function, as well as the technology providers that build and service these systems.
- Government's role is to protect its own systems; to ensure private entities, particularly critical infrastructure, are protecting their systems; and to carry out core government functions such a diplomacy, collecting intelligence, imposing economic costs, enforcing the law, and conducting disruptive actions to counter cyber threats.
- Industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society's most vulnerable, and defend our shared digital ecosystem.

Shift #2: Realign Incentives to Favor Long-Term Investments

- Our economy & society must incentivize decision-making to make cyberspace more resilient and defensible over the long term.
- This strategy outlines how the Federal Government will use all tools available to reshape incentives and achieve unity of effort in a collaborative, equitable, and mutually beneficial manner
- Must ensure market forces and public programs:
  - Reward security and resilience
  - Build a robust and diverse cyber workforce
  - Embrace security and resilience by design
  - Strategically coordinate research and development investments in cybersecurity; and
  - Promote the collaborative stewardship of our digital ecosystem
- The Federal Government is making generational investments in renewing our infrastructure, digitizing and decarbonizing our energy systems, securing our semiconductor supply chains, modernizing our cryptographic technologies, and rejuvenating our foreign and domestic policy priorities.

Building on Existing Policy

- Strategy builds on work of prior administrations and other efforts by current administration.
- Developed alongside National Security Strategy and National Defense Strategy by broad interagency team and through a months-long consultation process with private sector and civil society.
- Informed by and implements values to realize a democratic vision for our digital ecosystem.
- Carries forward direction from Executive Orders.
- Integrates cybersecurity into once-in-a-generation new investments (Infrastructure Law, Inflation Reduction Act, CHIPS, EO 14017 (Supply Chains))

<table>
<tr><th colspan="2">Pillar 1. Defend Critical Infrastructure</th></tr>
<tr><td colspan="2">• Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity.
• Collaboration to address advanced threats will only be effective if owners and operators of critical infrastructure have cybersecurity protections in place to make it harder for adversaries to disrupt them.
• The Federal Government can better support the defense of critical infrastructure by making its own systems more defensible and resilient. This Administration is committed to improving Federal cybersecurity through long-term efforts to implement a zero-trust architecture strategy and modernize IT and OT infrastructure.</td></tr>
<tr><th>Strategic Objective</th><th>Lines of Effort</th></tr>
<tr><td rowspan="3"><i>1.1 Establish Cybersecurity Requirements to Support National Security and Public Safety</i></td><td>• Establish Cybersecurity Requirements to Secure Critical Infrastructure
– The Federal Government will use existing authorities to set necessary cybersecurity requirements in critical sectors.
– Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance and be agile enough to adapt as adversaries increase their capabilities and change their tactics.
– Regulators are encouraged to drive the adoption of secure-by design principles, prioritize the availability of essential services, and ensure that systems are designed to fail safely and recover quickly.
– Cloud-based services enable better and more economical cybersecurity practices at scale, but they are also essential to operational resilience across many critical infrastructure sectors.</td></tr>
<tr><td>• Harmonize and Streamline New and Existing Regulation
– Effective regulations minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets.
– Where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms.
– The Cyber Incident Reporting Council will coordinate, deconflict, and harmonize Federal incident reporting requirements.</td></tr>
<tr><td>• Enable Regulated Entities to Afford Security
– Different critical infrastructure sectors have varying capacities to absorb the costs of cybersecurity, ranging from low-margin sectors that cannot easily increase investment without intervention, to those where the marginal costs of improving cybersecurity can be absorbed.
– In some sectors, regulation may be necessary to create a level playing field so that companies are not trapped in a competition to underspend their peers on cybersecurity. In other sectors, regulators are encouraged to ensure that necessary investments in cybersecurity are incentivized through the rate-making process, tax structures, or other mechanisms.
– In setting new cybersecurity requirements, regulators are encouraged to consult with regulated entities to understand how those requirements will be resourced.</td></tr>
</table>

Strategic Objective	Lines of Effort
1.2 Scale Public-Private Collaboration	• Defending critical infrastructure against adversarial activity and other threats requires a model of cyber defense that emulates the distributed structure of the Internet. • We will realize this distributed, networked model by developing and strengthening collaboration between defenders through structured roles and responsibilities and increased connectivity enabled by the automated exchange of data, information, and knowledge. • CISA is the national coordinator for critical infrastructure security and resilience. In this role, CISA coordinates with Sector Risk Management Agencies (SRMAs) to enable the Federal Government to scale its coordination with critical infrastructure owners and operators across the United States. SRMAs have day-to-day responsibility and sector-specific expertise to improve security and resilience within their sectors. • SRMAs support individual owners and operators in their respective sectors who are responsible for protecting the systems and assets they operate. Information sharing and analysis organizations (ISAOs), sector-focused information sharing and analysis centers (ISACs), and similar organizations facilitate cyber defense operations across vast and complex sectors. • The Federal Government will collaborate with industry to define sector-by-sector needs and assess gaps in current SRMA capabilities. • We must complement human-to-human collaboration efforts with machine-to-machine data sharing and security orchestration. Realizing this model will enable real-time, actionable, and multi-directional sharing to drive threat response at machine speed.
1.3 Integrate Federal Cybersecurity Centers	• Federal Cybersecurity Centers serve as collaborative nodes that fuse whole-of-government capabilities across homeland defense, law enforcement, intelligence, diplomatic, economic, and military missions. • Once fully integrated, they will drive intragovernmental coordination and enable the Federal Government to effectively and decisively support non-Federal partners. • ONCD will lead the Administration's efforts to enhance integration of centers such as these, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale.
1.4 Update Federal Incident Response Plans and Processes	• The private sector is capable of mitigating most cyber incidents without direct Federal assistance. • When Federal assistance is required, the Federal Government must present a unified, coordinated, whole-of-government response. • The Federal Government must provide clear guidance on how private sector partners can reach Federal agencies for support during cyber incidents and what support the Federal Government may provide. • CISA will lead a process to update the subordinate National Cyber Incident Response Plan (NCIRP) to strengthen processes, procedures, and systems to more fully realize "a call to one is a call to all." • Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will enhance our awareness and ability to respond effectively. CIRCIA will require covered entities in critical infrastructure sectors to report covered cyber incidents to CISA within hours. • Following major incidents, we will ensure that the cybersecurity community benefits from lessons learned through the Cyber Safety Review Board (CSRB). • The Administration will work with Congress to pass legislation to codify the CSRB within DHS and provide it the authorities it needs to carry out comprehensive reviews of significant incidents.

Strategic Objective	Lines of Effort
1.5 Modernize Federal Defenses	• Collectively Defend Federal Civilian Agencies – Federal civilian executive branch (FCEB) agencies are responsible for managing and securing their own IT and OT systems. With different agency structures, missions, capabilities, and resourcing, FCEB cybersecurity outcomes vary. – We will continue to build Federal cohesion through focused action across the Federal Government. OMB, in coordination with CISA, will develop a plan of action to secure FCEB systems through collective operational defense, expanded availability of centralized shared services, and software supply chain risk mitigation. – These efforts will build on prior programs and prioritize actions that advance a whole-of-government approach to defending FCEB information systems.
	• Modernize Federal Systems – The Federal Government must replace or update IT and OT systems that are not defensible against sophisticated cyber threats. – The OMB zero trust architecture strategy directs FCEB agencies to implement multi-factor authentication, encrypt their data, gain visibility into their entire attack surface, manage authorization and access, and adopt cloud security tools. – OMB will lead development of a multi-year lifecycle plan to accelerate FCEB technology modernization, prioritizing Federal efforts on eliminating legacy systems which are costly to maintain and difficult to defend. – Replacing legacy systems with more secure technology, including through accelerating migration to cloud-based services, will elevate the cybersecurity posture across the Federal Government and, in turn, improve the security and resilience of the digital services it provides to the American people.
	• Defend National Security Systems – National security systems (NSS) store and process some of the Federal Government's most sensitive data and must be secured against a wide range of cyber and physical threats, including insider threats, cyber criminals, and the most sophisticated nation-state adversaries. – The Director of the NSA, as the National Manager for NSS, will coordinate with OMB to develop a plan for NSS at FCEB agencies that ensures implementation of the enhanced cybersecurity requirements of NSM-8.

Pillar 2. Disrupt and Dismantle Threat Actors

- The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests.
- Coordinated efforts by Federal and non-Federal entities have proven effective in frustrating the malicious cyber activity of foreign government, criminal, and other threat actors.
- Our efforts will require greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries use of U.S.-based infrastructure, and thwart global ransomware campaigns.

Strategic Objective	**Lines of Effort**
2.1 Integrate Federal Disruption Activities	• Disruption campaigns must become so sustained and targeted that criminal cyber activity is rendered unprofitable and foreign government actors engaging in malicious cyber activity no longer see it as an effective means of achieving their goals. • The Department of Defense's strategic approach of defending forward has helped generate insights on threat actors, identify and expose malware, and disrupt malicious activity before it could affect its intended targets. • DoD will develop an updated departmental cyber strategy aligned with the National Security Strategy, National Defense Strategy, and this National Cybersecurity Strategy. • DoD's new strategy will clarify how U.S. Cyber Command and other DoD components will integrate cyberspace operations into their efforts to defend against state and non-state actors capable of posing strategic-level threats to U.S. interests, while continuing to strengthen their integration and coordination of operations with civilian, law enforcement, and intelligence partners to disrupt malicious activity at scale. • The NCIJTF, as a multi-agency focal point for coordinating whole-of-government disruption campaigns, will expand its capacity to coordinate takedown and disruption campaigns with greater speed, scale, and frequency.
2.2 Enhance Public-Private Operational Collaboration to Disrupt Adversaries	• Effective disruption of malicious cyber activity requires more routine collaboration between the private sector entities that have unique insights and capabilities and the Federal agencies that have the means and authorities to act. • The 2021 takedown of the Emotet botnet showed the potential of this collaborative approach, with Federal agencies, international allies and partners, and private industry cooperating to disrupt the botnet's operations. • Private sector partners are encouraged to come together and organize their efforts through one or more nonprofit organizations that can serve as hubs for operational collaboration with the Federal Government, such as the National Cyber-Forensics and Training Alliance (NCFTA). • The Federal Government will rapidly overcome barriers to supporting and leveraging this collaboration model, such as security requirements and records management policy.
2.3 Increase the Speed and Scale of Intelligence Sharing and Victim Notification	• The timely sharing of threat intelligence between Federal and non-Federal partners enhances collaborative efforts to disrupt and dismantle adversaries. • Open-source cybersecurity intelligence and private sector intelligence providers have greatly increased collective awareness of cyber threats, but national intelligence that only the government can collect remains invaluable. • The Federal Government will increase the speed and scale of cyber threat intelligence sharing to proactively warn cyber defenders and notify victims when the government has information that an organization is being actively targeted or may already be compromised. • SRMAs, in coordination with CISA, law enforcement agencies, and the CTIIC, will identify intelligence needs and priorities within their sector and develop processes to share warnings, technical indicators, threat context, and other relevant information with both government and non-government partners. • The Federal Government will also review declassification policies and processes to determine the conditions under which extending additional classified access and expanding clearances is necessary to provide actionable intelligence to owners and operators of critical infrastructure.

Strategic Objective	**Lines of Effort**
2.4 Prevent Abuse of U.S.-Based Infrastructure	• Malicious cyber actors exploit U.S.-based cloud infrastructure, domain registrars, hosting and email providers, and other digital services to carry out criminal activity, malign influence operations, and espionage against individual victims, businesses, governments, and other organizations in the United States and abroad. • The Federal Government will work with cloud and other internet infrastructure providers to quickly identify malicious use of U.S.-based infrastructure, share reports of malicious use with the government, make it easier for victims to report abuse of these systems, and make it more difficult for malicious actors to gain access to these resources in the first place. • All service providers must make reasonable attempts to secure the use of their infrastructure against abuse or other criminal behavior. • The Administration will prioritize adoption and enforcement of a risk-based approach to cybersecurity across Infrastructure-as-a-Service providers that addresses known methods and indicators of malicious activity including through implementation of EO • 13984, “Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.”
2.5 Counter Cybercrime, Defeat Ransomware	• Ransomware is a threat to national security, public safety, and economic prosperity. • United States will employ all elements of national power to counter the threat along four lines of effort: – leveraging international cooperation to disrupt the ransomware ecosystem and isolate those countries that provide safe havens for criminals; – investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors; – bolstering critical infrastructure resilience to withstand ransomware attacks; and – addressing the abuse of virtual currency to launder ransom payments. • The Joint Ransomware Task Force (JRTF), co-chaired by CISA and the Federal Bureau of Investigation (FBI), will coordinate, deconflict, and synchronize existing interagency efforts to disrupt ransomware operations and provide support to private sector and SLTT efforts to increase their protections against ransomware. • Our approach will also include targeting the illicit cryptocurrency exchanges on which ransomware operators rely and improving international implementation of standards for combatting virtual asset illicit finance. • the most effective way to undermine the motivation of these criminal groups is to reduce the potential for profit. For this reason, the Administration strongly discourages the payment of ransoms. At the same time, victims of ransomware – whether or not they choose to pay a ransom - should report the incident to law enforcement and other appropriate agencies.

<table>
<tr><th colspan="2">Pillar 3. Shape Market Forces to Drive Security and Resilience</th></tr>
<tr><td colspan="2">• To build the secure and resilient future we want, we must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk.
• Our goal is a modern digital economy that promotes practices that enhance the security and resilience of our digital ecosystem while preserving innovation and competition.
• Continued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience.
• To address these challenges, the Administration will shape the long-term security and resilience of the digital ecosystem, against both today’s threats and tomorrow’s challenges.
• We must hold the stewards of our data accountable for the protection of personal data; drive the development of more secure connected devices; and reshape laws that govern liability for data losses and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies.</td></tr>
<tr><th>Strategic Objective</th><th>Lines of Effort</th></tr>
<tr><td><i>3.1 Hold the Stewards of Data Accountable</i></td><td>• Securing personal data is a foundational aspect to protecting consumer privacy in a digital future.
• The Administration supports legislative efforts to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data and provide strong protections for sensitive data like geolocation and health information.
• This legislation should also set national requirements to secure personal data consistent with standards and guidelines developed by NIST.</td></tr>
<tr><td><i>3.2 Drive the Development of Secure IoT Devices</i></td><td>• Internet of Things (IoT) devices, including both consumer goods like fitness trackers and baby monitors, as well as industrial control systems and sensors, introduce new sources of connectivity in our homes and businesses.
• Many of the IoT devices deployed today are not sufficiently protected against cybersecurity threats. Too often they have been deployed with inadequate default settings, can be difficult or impossible to patch or upgrade, or come equipped with advanced—and sometimes unnecessary—capabilities that enable malicious cyber activities on critical physical and digital systems.
• Administration will continue to advance the development of IoT security labeling programs, as directed under EO 14028, “Improving the Nation’s Cybersecurity.”</td></tr>
<tr><td><i>3.3 Shift Liability for Insecure Software Products and Services</i></td><td>• Markets impose inadequate costs on—and often reward—those entities that introduce vulnerable products or services into our digital ecosystem.
• Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance.
• Software makers are able to leverage their market position to fully disclaim liability by contract, further reducing their incentive to follow secure-by-design principles or perform pre-release testing.
• We must begin to shift liability onto entities that fail to take reasonable precautions to secure their software while recognizing even the most advanced software security programs cannot prevent all vulnerabilities.
• The Administration will work with Congress and the private sector to develop legislation establishing liability for software products and services. Any such legislation should prevent manufacturers and software publishers with market power from fully disclaiming liability by contract, and establish higher standards of care for software in specific high-risk scenarios.
• The Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services.
• To further incentivize the adoption of secure software development practices, the Administration will encourage coordinated vulnerability disclosure across all technology types and sectors; promote the further development of SBOMs; and develop a process for identifying and mitigating the risk presented by unsupported software that is widely used or supports critical infrastructure.</td></tr>
</table>

Strategic Objective	**Lines of Effort**
3.4 Use Federal Grants and Other Incentives to Build in Security	• Federal grant programs offer strategic opportunities to make investments in critical infrastructure that are designed, developed, fielded, and maintained with cybersecurity and all-hazards resilience in mind. • The Federal Government will collaborate with SLTT entities, the private sector, and other partners to balance cybersecurity requirements for applicants with technical assistance and other forms of support. • The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience.
3.5 Leverage Federal Procurement to Improve Accountability	• Contracting requirements for vendors that sell to the Federal Government have been an effective tool for improving cybersecurity. • The Civil Cyber-Fraud Initiative (CCFI) uses DOJ authorities under the False Claims Act to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations. The CCFI will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cyber incidents and breaches.
3.6 Explore a Federal Cyber Insurance Backstop	• When catastrophic incidents occur, it is a government responsibility to stabilize the economy and provide certainty in uncertain times. • The Administration will assess the need for and possible structures of a Federal insurance response to catastrophic cyber events that would support the existing cyber insurance market.

Pillar 4. Invest in a Resilient Future

- We can build a more secure, resilient, privacy-preserving, and equitable digital ecosystem through strategic investments and coordinated, collaborative action.
- Foundational elements of our digital ecosystem, like the Internet, are products of sustained and mutually-supporting investments by both public and private sector entities.
- The Federal Government must leverage strategic public investments in innovation, R&D, and education to drive outcomes that are economically sustainable and serve the national interest.
- Decades of adversaries and malicious actors weaponizing our technology and innovation against us—to steal our intellectual property, interfere in or influence our electoral process, and undercut our national defenses—has demonstrated that leadership in innovation without security is not enough.
- We will ensure that resilience is not a discretionary element of new technical capabilities but a commercially viable element of the innovation and deployment process.

Strategic Objective	**Lines of Effort**
4.1 Secure the Technical Foundations of the Internet	• The Internet is critical to our future but retains the fundamental structure of its past. Many of the technical foundations of the digital ecosystem are inherently vulnerable. Every time we build something new on top of this foundation, we add new vulnerabilities and increase our collective risk exposure. • We must take steps to mitigate the most urgent of these pervasive concerns such as Border Gateway Protocol vulnerabilities, unencrypted Domain Name System requests, and the slow adoption of IPv6. • Such a "clean-up" effort to reduce systemic risk requires identification of the most pressing of these security challenges, further development of effective security measures, and close collaboration between public and private sectors to reduce our risk exposure without disrupting the platforms and services built atop this infrastructure. • Preserving and extending the open, free, global, interoperable, reliable, and secure Internet requires sustained engagement in standards development processes to instill our values and ensure that technical standards produce technologies that are more secure and resilient. • As autocratic regimes seek to change the Internet and its multi-stakeholder foundation to enable government control, censorship, and surveillance, the United States and its foreign and private sector partners will implement a multi-pronged strategy to preserve technical excellence, protect our security, drive economic competitiveness, promote digital trade, and ensure that the "rules of the road" for technology standards favor principles of transparency, openness, consensus, relevance, and coherence.
4.2 Reinvigorate Federal Research and Development for Cybersecurity	• Through Federal efforts to prioritize research and development in defensible and resilient architectures and reduce vulnerabilities in underlying technologies, we can ensure that the technologies of tomorrow are more secure than those of today. • The Federal Government will identify, prioritize, and catalyze the research, development, and demonstration (RD&D) community to proactively prevent and mitigate cybersecurity risks in existing and next generation technologies. • Departments and agencies will direct RD&D projects to advance cybersecurity and resilience in areas such as artificial intelligence, operational technologies and industrial control systems, cloud infrastructure, telecommunications, encryption, system transparency, and data analytics used in critical infrastructure. • These RD&D investments will focus on securing three families of technologies that will prove decisive for U.S. leadership in the coming decade: computing-related technologies, including microelectronics, quantum information systems, and artificial intelligence; biotechnologies and biomanufacturing; and clean energy technologies.
4.3 Prepare for our Post-Quantum Future	• Strong encryption is foundational to cybersecurity and global commerce. It is the primary way we protect our data online, validate end users, authenticate signatures, and certify the accuracy of information. • Quantum computing has the potential to break some of the most ubiquitous encryption standards deployed today. • The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum resistant cryptography-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Strategic Objective	**Lines of Effort**
4.4 Secure our Clean Energy Future	• Our accelerating national transition to a clean energy future is bringing online a new generation of interconnected hardware and software systems that have the potential to strengthen the resiliency, safety, and efficiency of the U.S. electric grid. • These technologies, including distributed energy resources, "smart" energy generation and storage devices, advanced cloud-based grid management platforms, and transmission and distribution networks designed for high-capacity controllable loads are far more sophisticated, automated, and digitally interconnected than prior generations of grid systems. • The Administration will seize this strategic opportunity to build in cybersecurity proactively through implementation of the Congressionally-directed National Cyber-Informed Engineering Strategy, rather than developing a patchwork of security controls after these connected devices are widely deployed. • DOE will also continue to promote cybersecurity for electric distribution and distributed energy resources in partnership with industry, States, Federal regulators, Congress, and other agencies.
4.5 Support Development of a Digital Identity Ecosystem	• Enhanced digital identity solutions and infrastructure can enable a more innovative, equitable, safe and efficient digital economy. • Today, the lack of secure, privacy-preserving, consent-based digital identity solutions allows fraud to flourish, perpetuates exclusion and inequity, and adds inefficiency to financial activities and daily life. • The Federal Government will encourage and enable investments in strong, verifiable digital identity solutions that promote security, accessibility and interoperability, financial and social inclusion, consumer privacy, and economic growth. • Acknowledging that States are piloting mobile drivers' licenses, we note and encourage a focus on privacy, security, civil liberties, equity, accessibility, and interoperability.
4.6 Develop a National Strategy to Strengthen our Cyber Workforce	• Today, there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide, and this gap is growing. • To address this challenge, ONCD will lead the development and oversee implementation of a National Cyber Workforce and Education Strategy. – This strategy will take a comprehensive and coordinated approach to expanding the national cyber workforce, improving its diversity, and increasing access to cyber educational and training pathways. – It will address the need for cybersecurity expertise across all sectors of the economy, with a special focus on critical infrastructure, and will enable the American workforce to continue to innovate in secure and resilient next-generation technologies. – The strategy will strengthen and diversify the Federal cyber workforce, addressing the unique challenges the public sector faces in recruiting, retaining, and developing the talent and capacity needed to protect Federal data and IT infrastructure. – The strategy will recognize that cyber workforce challenges are not unique to the United States, expanding upon and drawing inspiration from efforts underway in other countries. – The strategy will build on existing efforts to develop our national cybersecurity workforce including the National Initiative for Cybersecurity Education (NICE), the CyberCorps: Scholarship for Service program, the National Centers of Academic Excellence in Cybersecurity program, the Cybersecurity Education Training and Assistance Program, and the registered apprenticeships program. – The strategy will also leverage ongoing workforce development programs at NSF and other science agencies to augment Federal Government programs. – It will tackle head on the lack of diversity in the cyber workforce. Addressing systemic inequities and overcoming barriers that inhibit diversity in the cyber workforce is both a moral necessity and a strategic imperative. • To recruit and train the next generation of cybersecurity professionals to secure our digital ecosystem will require Federal leadership and enduring partnership between public and private sectors. Building and maintaining a strong cyber workforce cannot be achieved unless a cybersecurity career is within reach for any capable American who wishes to pursue it and every organization with an unfilled position plays a part in training the next generation of cybersecurity talent.

Pillar 5. Forge International Partnerships to Pursue Shared Goals

- The United States seeks a world where responsible state behavior in cyberspace is expected and rewarded and where irresponsible behavior is isolating and costly.
- To achieve this goal, we will continue to engage with countries working in opposition to our larger agenda on common problems while we build a broad coalition of nations working to maintain an open, free, global, interoperable, reliable, and secure Internet.
- To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community.
- We will expand coalitions, collaboratively disrupt transnational criminals and other malicious cyber actors, build the capacity of our international allies and partners, reinforce the applicability of existing international law to state behavior in cyberspace, uphold globally accepted and voluntary norms of responsible state behavior in peacetime, and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

Strategic Objective	**Lines of Effort**
5.1 Build Coalitions to Counter Threats to Our Digital Ecosystem	• In April 2022, the United States and 60 countries launched the Declaration for the Future of the Internet (DFI), bringing together a broad, diverse coalition of partners—the largest of its kind— around a common, democratic vision for an open, free, global, interoperable, reliable, and secure digital future. • Through mechanisms like the Quadrilateral Security Dialogue (“the Quad”) between the United States, India, Japan, and Australia, the United States and its international allies and partners are advancing these shared goals for cyberspace. • These include improving information sharing between computer emergency response teams and the development of a digital ecosystem based on shared values. • Through these and other partnerships, the United States and international counterparts can advance common cybersecurity interests by sharing cyber threat information, exchanging model cybersecurity practices, comparing sector-specific expertise, driving secure-by-design principles, and coordinating policy and incident response activities. • Because most malicious cyber activity targeting the United States is carried out by actors based in foreign countries or using foreign computing infrastructure, we must strengthen the mechanisms we have to collaborate with our allies and partners so that no adversary can evade the rule of law.
5.2 Strengthen International Partner Capacity	• As we build a coalition to advance shared cybersecurity priorities and promote a common vision for the digital ecosystem, the United States will strengthen the capacity of like-minded states across the globe to support these goals. • We must enable our allies and partners to – secure critical infrastructure networks, – build effective incident detection and response capabilities, – share cyber threat information, – pursue diplomatic collaboration, – build law enforcement capacity and effectiveness through operational collaboration, – and support our shared interests in cyberspace by adhering to international law and reinforcing norms of responsible state behavior. • To accomplish this goal, the United States will marshal expertise across agencies, the public and private sectors, and among advanced regional partners to pursue coordinated and effective international cyber capacity-building and operational collaboration efforts. – DOJ will continue to build a more robust cybercrime cooperation paradigm through bilateral and multilateral engagement and agreements, formal and informal cooperation, and providing international and regional leadership to strengthen cybercrime laws, policies, and operations. – DoD will continue to strengthen its military-to-military relationships to leverage allies’ and partners’ unique skills and perspectives while building their capacity to contribute to our collective cybersecurity posture. – Department of State will continue to coordinate whole-of-government efforts to ensure Federal capacity building priorities are strategically aligned and further U.S., allied, and partner interests.

Strategic Objective	**Lines of Effort**
5.3 Expand U.S. Ability to Assist Allies and Partners	• Allies and partners who fall victim to a significant cyberattack may seek support from the United States and allied and partner nations to investigate, responding to, and recover from such incidents. • Providing this support will not only assist with partner recovery and response, but will also advance U.S. foreign policy and cybersecurity goals. • Close cooperation with an affected ally or partner demonstrates solidarity in the face of adversary activity and can accelerate efforts to expose counter-normative state behavior and impose consequences. • The Administration will establish policies for determining when it is in the national interest to provide such support, develop mechanisms for identifying and deploying department and agency resources in such efforts, and, where needed, rapidly seek to remove existing financial and procedural barriers to provide such operational support.
5.4 Build Coalitions to Reinforce Global Norms of Responsible State Behavior	• Every member of the United Nations has made a political commitment to endorse peacetime norms of responsible state behavior in cyberspace that includes refraining from cyber operations that would intentionally damage critical infrastructure contrary to their obligations under international law. • While our adversaries know that such commitments are not self-enforcing, the growing influence of this framework has led states to call out those who act contrary to it. • The United States, as a core part of its renewed, active diplomacy, will hold irresponsible states accountable when they fail to uphold their commitments. • To effectively constrain our adversaries and counter malicious activities below the threshold of armed conflict, we will work with our allies and partners to pair statements of condemnation with the imposition of meaningful consequences
5.5 Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services	• Complex and globally interconnected supply chains produce the information, communications, and operational technology products and services that power the U.S. economy. • From raw materials and basic components to finished products and services—both virtual and physical—we depend upon a growing network of foreign suppliers. • This dependency on critical foreign products and services from untrusted suppliers introduces multiple sources of systemic risk to our digital ecosystem. • Mitigating this risk will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more transparent, secure, resilient, and trustworthy. • Critical inputs, components, and systems must increasingly be developed at home or in close coordination with allies and partners who share our vision of an open, free, global, interoperable, reliable, and secure Internet. – 5G Example Open Radio Access Networks (Open RAN)) • The United States will work with our allies and partners, including through regional partnerships like IPEF, the Quad Critical and Emerging Technology Working Group, and the TTC, to identify and implement best practices in cross-border supply chain risk management and work to shift supply chains to flow through partner countries and trusted vendors.

Implementation

Assessing Effectiveness

- Data-driven approach.
- Measure investments made, progress towards implementation, and ultimate outcomes and effectiveness.
- ONCD will assess effectiveness and report annually to the President.

Incorporating Lessons Learned

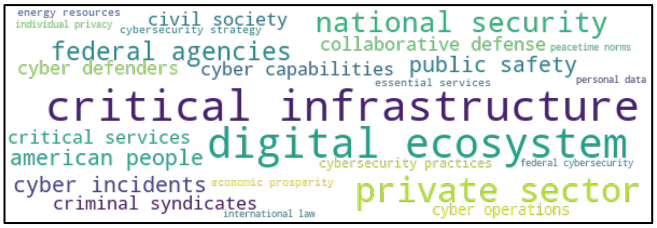
- Federal Government will prioritize capturing lessons learned from cyber incidents and apply those lessons in the implementation of this strategy.
- CSRB provided industry, Federal agencies, and the software development community with clear, actionable recommendation from their review of Log4j.
- A broader nation effort to learn from cyber incidents is required.
- Regulators are encouraged to build incident review processes into their frameworks.
  - CISA and law enforcement agencies are also encouraged to build processes to routinely extract lessons learned from their investigations and incident response activities.
  - Private companies are likewise encouraged to undertake these reviews and share findings from their efforts to inform implementation of this strategy.

Making the Investment

- Maintaining an open, free, global, interoperable, reliable, and secure Internet and building a more defensible and resilient digital ecosystem will require generational investments by the Fed allies and partners, and by the private sector.
  - Many Federal actions contained in this strategy are intended to increase private sector investment in security, resilience, improved collaboration, and research and development.
  - For Federal agencies to support their private sector partners and increase their capacity to carry out essential Federal missions, targeted investments will be required.
  - ONCD and OMB will jointly issue annual guidance on cybersecurity budget priorities
  - ONCD will work with OMB to ensure alignment of department and agency budget proposals to achieve the goals set out in this strategy.
  - The Administration will work with Congress to fund cybersecurity activities to keep pace with the speed of changed inherent within the cyber ecosystem.

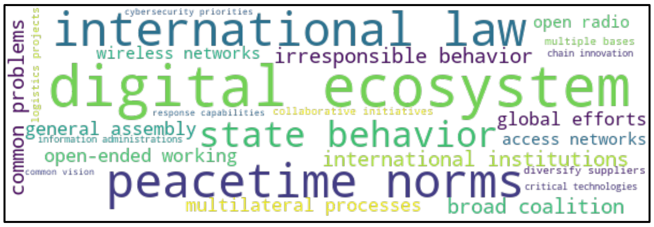
Sample IDATA-generated Artifacts[2]

Word Cloud

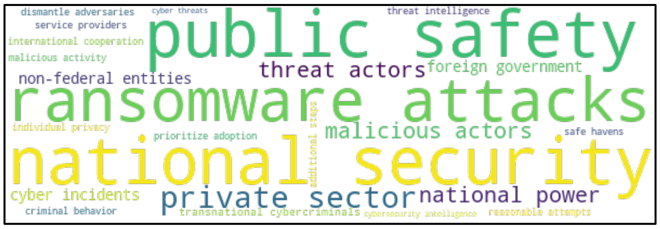


Themes

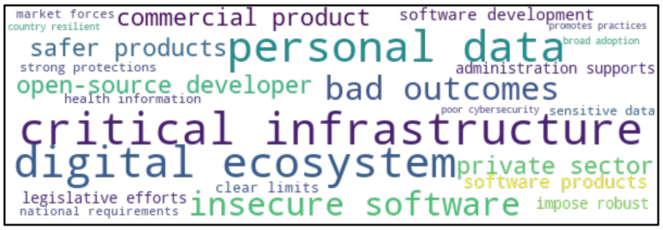
international partnerships and coalitions



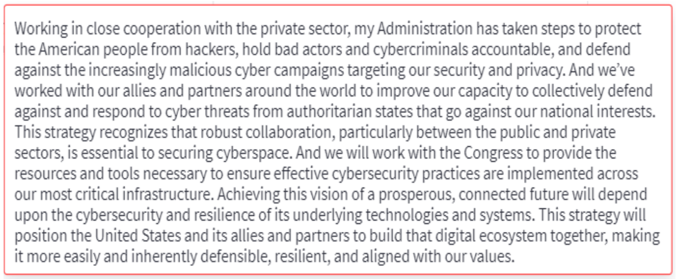
threat actors and malicious activities



infrastructure/software/products



IDATA Computed Summary



Working in close cooperation with the private sector, my Administration has taken steps to protect the American people from hackers, hold bad actors and cybercriminals accountable, and defend against the increasingly malicious cyber campaigns targeting our security and privacy. And we've worked with our allies and partners around the world to improve our capacity to collectively defend against and respond to cyber threats from authoritarian states that go against our national interests. This strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace. And we will work with the Congress to provide the resources and tools necessary to ensure effective cybersecurity practices are implemented across our most critical infrastructure. Achieving this vision of a prosperous, connected future will depend upon the cybersecurity and resilience of its underlying technologies and systems. This strategy will position the United States and its allies and partners to build that digital ecosystem together, making it more easily and inherently defensible, resilient, and aligned with our values.

Similarity Analysis: EO 14028 (Cybersecurity) Sections to National Cybersecurity Strategy Strategic Objectives (SO)

Top 3 Most Similar Strategic Objectives in Each Section:

EO: Section 1. Policy

SO 2.4: Prevent Abuse of U.S.-Based Infrastructure
SO 2.1: Integrate Federal Disruption Activities
SO 1.1: Establish Cybersecurity Requirements to Support National Security and Public Safety

EO: Sec. 2. Removing Barriers to Sharing Threat Information

SO 2.3: Increase the Speed and Scale of Intelligence Sharing and Victim Notification
SO 2.4: Prevent Abuse of U.S.-Based Infrastructure
SO 1.4: Update Federal Incident Response Plans and Processes

EO: Sec. 3. Modernizing Federal Government Cybersecurity

SO 1.5: Modernize Federal Defenses
SO 3.4: Use Federal Grants and Other Incentives to Build in Security
SO 4.2: Reinvigorate Federal Research and Development for Cybersecurity

EO: Sec. 4. Enhancing Software Supply Chain Security

SO 3.3: Shift Liability for Insecure Software Products and Services
SO 3.5: Leverage Federal Procurement to Improve Accountability
SO 1.5: Modernize Federal Defenses

EO: Sec. 5. Establishing a Cyber Safety Review Board

SO 1.4: Update Federal Incident Response Plans and Processes
SO 5.3: Expand U.S. Ability to Assist Allies and Partners
SO 2.1: Integrate Federal Disruption Activities

EO: Sec. 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents

SO 1.4: Update Federal Incident Response Plans and Processes
SO 1.5: Modernize Federal Defenses
SO 2.1: Integrate Federal Disruption Activities

EO: Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

SO 1.5: Modernize Federal Defenses
SO 1.4: Update Federal Incident Response Plans and Processes
SO 1.3: Integrate Federal Cybersecurity Centers

EO: Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities

SO 1.4: Update Federal Incident Response Plans and Processes
SO 1.5: Modernize Federal Defenses
SO 3.1: Hold the Stewards of Our Data Accountable

EO: Sec. 9. National Security Systems

SO 1.5: Modernize Federal Defenses
SO 1.4: Update Federal Incident Response Plans and Processes
SO 2.1: Integrate Federal Disruption Activities

[2] IDATA is an internal IDA natural language processing and data analysis capability

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number**. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY) 00-03-23	2. REPORT TYPE Non-Standard	3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE Summary of National Cybersecurity Strategy with Similarity Analysis to Executive Order 14028, “Improving the Nation’s Cybersecurity”	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS
6. AUTHOR(S) Kevin Garrison, Pranay N. Bhandare, Travis L. DePriest, Katharina M. Gallmeier, Arun S. Maiya	5d. PROJECT NUMBER C5107
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	8. PERFORMING ORGANIZATION REPORT NUMBER NS D-33439
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	10. SPONSOR’S / MONITOR’S ACRONYM IDA
	11. SPONSOR’S / MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.
13. SUPPLEMENTARY NOTES Project Leader: Kevin Garrison
14. ABSTRACT Provides a tabularized and shortened version of the National Cybersecurity Strategy (March 2023) along with analytical products that elucidate key themes and terms in the strategy, as well as an analysis of similarities to the May 2021 Executive Order about cybersecurity.
15. SUBJECT TERMS National policy, strategy, cybersecurity, economic wellbeing, democratic values

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Institute for Defense Analyses
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Unlimited	16	19b. TELEPHONE NUMBER (Include Area Code)