National Cybersecurity Strategy

MARCH 2023

THE WHITE HOUSE
WASHINGTON

THE WHITE HOUSE

WASHINGTON

March 1, 2023

Digital technologies today touch nearly every aspect of American life. The openness and connection enabled by access to the Internet are game-changers for communities everywhere, as we have all experienced throughout the COVID-19 pandemic. That's why, thanks to the Bipartisan Infrastructure Law, my Administration is investing $65 billion to make sure every American has access to reliable, high-speed Internet. And when we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the Internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable, and secure. This National Cybersecurity 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.

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. From the very beginning of my Administration, we have moved decisively to strengthen cybersecurity. I appointed senior cybersecurity officials at the White House and issued an Executive Order on Improving the Nation's Cybersecurity. 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. It also takes on the systemic challenge that too much of the responsibility for cybersecurity has fallen on individual users and small organizations. By working in partnership with industry; civil society; and State, local, Tribal, and territorial governments, we will rebalance the responsibility for cybersecurity to be more effective and more equitable. We will realign incentives to favor long-term investments in security, resilience, and promising new technologies. We will collaborate with our allies and partners to strengthen norms of responsible state behavior, hold countries accountable for irresponsible behavior in cyberspace, and disrupt the networks of criminals behind dangerous cyberattacks around the globe. 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.

As I have often said, our world is at an inflection point. That includes our digital world. The steps we take and choices we make today will determine the direction of our world for decades

to come. This is particularly true as we develop and enforce rules and norms for conduct in 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. Digital connectivity should be a tool that uplifts and empowers people everywhere, not one used for repression and coercion. As this strategy details, the United States is prepared to meet this challenge from a position of strength, leading in lockstep with our closest allies and working with partners everywhere who share our vision for a brighter digital future.

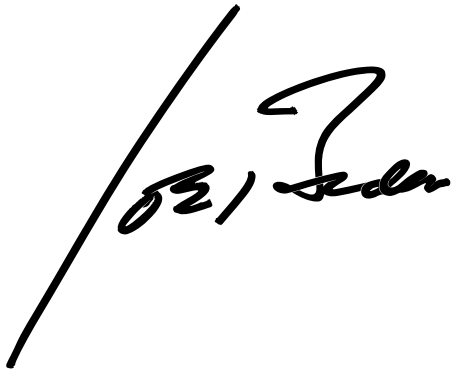

TABLE OF CONTENTS

INTRODUCTION

The Internet has transformed our world. In a single generation, it has revolutionized the way we innovate, communicate, and share information on a global scale, catalyzing unprecedented advancements in human prosperity, equality, and connectivity. Upon this Internet backbone we have built a flourishing digital ecosystem, combining systems and technologies with our economies, our societies, and ourselves.

In doing so, the digital ecosystem has come to reflect the values of its architects and its users. Technologies have promoted democracy, free speech, innovation, and equality. But they also have been misused to enable transnational repression and digital authoritarianism; steal data and intellectual property; distribute disinformation; disrupt critical infrastructure; proliferate online harassment, exploitation, and abuse; enable criminals and foster violent extremism; and threaten peace and stability. People and technology are increasingly linked, further enabling the very best, as well as the worst, of humanity.

In this decisive decade, we have grand ambitions for the further values-driven development of our digital ecosystem. We are building a smart grid, powered by distributed renewable electricity and balanced with intelligent systems, that promises a bright and resilient future of energy abundance. We envision a maturing "Internet of Things" (IoT), comprising everything from consumer goods to digitized industrial controls to constellations of satellites, that will increase efficiency and safety while providing game-changing insights into our environment and economy. We are laying the foundations for real-time global collaboration leveraging vast amounts of data and computing power that will unlock scientific discoveries and other public goods of which we cannot yet conceive.

Achieving this vision of a prosperous, connected future will depend upon the cybersecurity and resilience of its underlying technologies and systems. We have learned hard lessons and made significant progress in the collaborative defense of our digital ecosystem. Every day, cyber defenders foil state-backed attacks and prevent criminal plots around the world. But the underlying structural dynamics of the digital ecosystem frustrate their efforts. Its components remain prone to disruption, vulnerable to exploitation, and are often co-opted by malicious actors.

We must make fundamental changes to the underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it. Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences. In creating these conditions, we can and must seize the opportunity to instill our most cherished values, as embodied by the Declaration for the Future of the Internet (DFI) and by the Freedom Online Coalition.

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. By the end of this decisive decade, we will achieve these outcomes so we can confidently take bold leaps into a digitally-enabled future that benefits us all.

The Strategic Environment

The United States has made significant progress toward achieving the President's affirmative vision for a digitally-enabled future, but emerging trends are creating both new opportunities for further advancement and new challenges to overcome. Malicious actors threaten our progress toward a digital ecosystem that is inclusive, equitable, promotes prosperity, and aligns with our democratic values.

Emerging Trends

The world is entering a new phase of deepening digital dependencies. Driven by emerging technologies and ever more complex and interdependent systems, dramatic shifts in the coming decade will unlock new possibilities for human flourishing and prosperity while also multiplying the systemic risks posed by insecure systems.

Software and systems are growing more complex, providing value to companies and consumers but also increasing our collective insecurity. Too often, we are layering new functionality and technology onto already intricate and brittle systems at the expense of security and resilience. The widespread introduction of artificial intelligence systems—which can act in ways unexpected to even their own creators—is heightening the complexity and risk associated with many of our most important technological systems.

The Internet continues to connect individuals, businesses, communities, and countries on shared platforms that enable scaled business solutions and international exchange. But this accelerating global interconnectivity also introduces risks. An attack on one organization, sector, or state can rapidly spill over to other sectors and regions, as happened during Russia's 2017 "NotPetya" cyberattack on Ukraine, which spread across Europe, Asia, and the Americas, causing billions of dollars in damage. The potential cost of attacks like this will only grow as interdependencies increase.

Digital technologies increasingly touch the most sensitive aspects of our lives, providing convenience, but also creating new, often unforeseen risks. The COVID-19 pandemic has pushed us to live ever more deeply in a digital world. As our lives become intertwined with video and audio streaming, wearable devices, and biometric technologies, the quantity and intimacy of personal data collection is growing exponentially. Theft of that data is also growing rapidly, and opening up novel vectors for malicious actors to surveil, manipulate, and blackmail individuals.

Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing some of our most essential systems to disruption. Our factories, power grids, and water treatment facilities, among other essential infrastructure, are increasingly shedding old analog control systems and rapidly bringing online digital operational technology (OT). Advanced wireless technologies, IoT, and space-based assets—including those enabling positioning, navigation, and timing for civilian and military uses, environmental and weather monitoring, and everyday Internet-based activities from banking to telemedicine—will accelerate this trend, moving many of

our essential systems online and making cyberattacks inherently more destructive and impactful to our daily lives.

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 cyber-enabled influence campaigns designed to undermine public trust in the foundation of our democracy. Once available only to a small number of well-resourced countries, offensive hacking tools and services, including foreign commercial spyware, are now widely accessible. These tools and services empower countries that previously lacked the ability to harm U.S. interests in cyberspace and enable a growing threat from organized criminal syndicates.

The 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. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity.

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 intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. Over the last ten years, it has expanded cyber operations beyond intellectual property theft to become our most advanced strategic competitor with the capacity to threaten U.S. interests and dominate emerging technologies critical to global development. Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders.

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. Russia remains a persistent cyber threat as it refines its cyber espionage, attack, influence, and disinformation capabilities to coerce sovereign countries, harbor transnational criminal actors, weaken U.S. alliances and partnerships, and subvert the rules-based international system. Like its 2017 "NotPetya" attack, Russia's cyberattacks in support of its 2022 brutal and unprovoked invasion of Ukraine have resulted in irresponsible spillover impacts onto civilian critical infrastructure in other European countries.

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. Iran has used cyber capabilities to threaten U.S. allies in the Middle East and elsewhere, while the DPRK conducts cyber activities to generate revenue through criminal enterprises, such as through the theft of cryptocurrency, ransomware, and the deployment of surreptitious information technology (IT) workers for the purposes of fueling its nuclear ambitions. Further maturation of these capabilities could have significant impacts on U.S., allied, and partner interests.

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. Ransomware incidents have disrupted critical services and businesses across the country and around the world, from energy pipelines and food companies, to schools and hospitals. Total economic losses from ransomware attacks continue to climb, reaching billions of U.S. dollars annually. Criminal syndicates often operate out of states that do not cooperate with U.S. law enforcement and frequently encourage, harbor, or tolerate such activities. These and other malicious cyber activities continue to threaten Americans across society, including disproportionately affecting those without the resources necessary to protect themselves, recover, or seek recourse.

Our Approach: A Path to Resilience in Cyberspace

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. This strategy seeks to build and enhance collaboration around five pillars: (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, and (5) Forge International Partnerships to Pursue Shared Goals. Each effort 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 this vision, and identify strategic objectives around which to organize their efforts.

To realize the vision these pillars lay out, we will make **two fundamental shifts** in how the United States allocates roles, responsibilities, and resources in cyberspace. In realizing these shifts, we aspire not just to improve our defenses, but to change those underlying dynamics that currently contravene our interests.

Rebalance the Responsibility to Defend Cyberspace

The most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem. Today, end users bear too great a burden for mitigating cyber risks. Individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity. A single person's momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences. Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens.

Instead, across both the public and private sectors, we must ask more of the most capable and best-positioned actors to make our digital ecosystem secure and resilient. In a free and interconnected society, protecting data and assuring the reliability of critical systems must be the responsibility of the owners and operators of the systems that hold our data and make our society function, as well as

of 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 governmental functions such as engaging in diplomacy, collecting intelligence, imposing economic costs, enforcing the law, and, conducting disruptive actions to counter cyber threats. Together, 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.

Realign Incentives to Favor Long-Term Investments

Our economy and society must incentivize decision-making to make cyberspace more resilient and defensible over the long term. Balancing short-term imperatives against a long-term vision will be no easy task. We must defend the systems we have now, while investing in and building toward a future digital ecosystem that is more inherently defensible and resilient.

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. We must ensure that market forces and public programs alike 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. To achieve these goals, the Federal Government will focus on points of leverage, where minimally invasive actions will produce the greatest gains in defensibility and systemic resilience.

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. The United States has an opportunity to rebalance the incentives necessary to lay a stronger, more resilient foundation on which to build the future of our digital ecosystem.

Building on Existing Policy

This strategy, while laying out a new approach to our cybersecurity, builds on significant achievements already shaping our strategic environment and digital ecosystem. In its first days, the Biden-Harris Administration assumed responsibility for managing the fallout from Russia's compromise of the SolarWinds Orion platform and the PRC's compromise of servers running Microsoft Exchange. The President elevated White House leadership on cybersecurity, appointing experienced, senior leaders in new positions at the National Security Council (NSC) and the Office of National Cyber Director (ONCD), and moved quickly to fold lessons learned from these and other incidents into executive actions.

These forward-leaning efforts have laid the foundation upon which this strategy is built. It was developed alongside the National Security Strategy and National Defense Strategy by a broad

interagency team and through a months-long consultation process with the private sector and civil society. It is informed by and implements the values of the DFI, the Freedom Online Coalition, and other long-standing efforts to realize a democratic vision for our digital ecosystem. It carries forward the foundational direction of Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," National Security Memorandum (NSM) 5, "Improving Cybersecurity for Critical Infrastructure Control Systems," NSM 8, "Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems," and other executive actions. It integrates cybersecurity into the once-in-a-generation new investments made by the Bipartisan Infrastructure Law, the Inflation Reduction Act, the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, and EO 14017, "America's Supply Chains."

This strategy also builds on the work of prior administrations. It replaces the 2018 National Cyber Strategy but continues momentum on many of its priorities, including the collaborative defense of the digital ecosystem. The Administration remains committed to enhancing the security and resilience of U.S. space systems, including by implementing Space Policy Directive 5, "Cybersecurity Principles for Space Systems." The Administration also continues to implement critical efforts to secure next-generation technologies, including through the National Artificial Intelligence Initiative and the National Strategy to Secure 5G, among other existing policies and initiatives.

This strategy's goals for securing Federal systems and collaborating with the private sector build on EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," EO 13691, "Promoting Private Sector Cybersecurity Information Sharing," and EO 13636, "Improving Critical Infrastructure Cybersecurity," and fit within the frameworks established by Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," and Presidential Policy Directive 41, "United States Cyber Incident Coordination." It carries forward and evolves many of the strategic efforts originally initiated by the 2008 Comprehensive National Cybersecurity Initiative.

PILLAR ONE | DEFEND CRITICAL INFRASTRUCTURE

Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides. We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem.

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 Administration has established new cybersecurity requirements in certain critical sectors. In other sectors, new authorities will be required to set regulations that can drive better cybersecurity practices at scale. This Administration has conducted sector-specific engagement with industry to construct consistent, predictable regulatory frameworks for cybersecurity that focus on achieving security outcomes and enabling continuity of operations and functions, while promoting collaboration and innovation.

Private sector entities have made significant commitments to engage in collaborative defense efforts. The "Shields Up" campaign preceding Russia's 2022 brutal and unprovoked war on Ukraine, to proactively increase preparedness and promote effective measures to combat malicious activity, is an example of public-private collaboration that must be scaled and repeated.

We must build new and innovative capabilities that allow owners and operators of critical infrastructure, Federal agencies, product vendors and service providers, and other stakeholders to effectively collaborate with each other at speed and scale. Federal agencies that support critical infrastructure providers must enhance their own capabilities and their ability to collaborate with other Federal entities. When incidents occur, Federal response efforts must be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners.

Finally, 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. In doing so, Federal cybersecurity can be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems.

Strategic Objective 1.1: Establish Cybersecurity Requirements to Support National Security and Public Safety

The American people must have confidence in the critical services underpinning their lives and the nation's economy. While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. Today's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents.

Regulation can level the playing field, enabling healthy competition without sacrificing cybersecurity or operational resilience. Our strategic environment requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation. New and updated cybersecurity regulations must be calibrated to meet the needs of national security and public safety, in addition to the security and safety of individuals, regulated entities, and their employees, customers, operations, and data.

The Administration has made progress in this area, establishing cybersecurity requirements in key sectors such as oil and natural gas pipelines, aviation, and rail, led by the Transportation Security Administration and water systems, led by the Environmental Protection Agency. A collaborative process between industry and regulators will produce regulatory requirements that are operationally and commercially viable and will ensure the safe and resilient operation of critical infrastructure. The most effective and efficient regulatory frameworks will be those put in place well before a crisis, rather than through the imposition of emergency regulations after a crisis occurs.

Establish Cybersecurity Regulations to Secure Critical Infrastructure

The Federal Government will use existing authorities to set necessary cybersecurity requirements in critical sectors. Where Federal departments and agencies have gaps in statutory authorities to implement minimum cybersecurity requirements or mitigate related market failures, the Administration will work with Congress to close them. Where states or independent regulators have authorities that can be used to set cybersecurity requirements, the Administration will encourage them to use those authorities in a deliberate and coordinated manner.

Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance—including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity— and be agile enough to adapt as adversaries increase their capabilities and change their tactics. In setting cybersecurity regulations for critical infrastructure, 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. Regulations will define minimum expected cybersecurity practices or outcomes, but the Administration encourages and will support further efforts by entities to exceed these requirements.

Further, these and other critical sectors rely upon the cybersecurity and resilience of their third-party service providers. 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. The Administration will identify gaps in authorities to drive better cybersecurity practices in the cloud computing industry and for other essential third-party services, and work with industry, Congress, and regulators to close them.

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. By leveraging existing international standards in a manner consistent with current policy and law, regulatory agencies can minimize the burden of unique requirements and reduce the need for regulatory harmonization.

Where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms. When necessary, the United States will pursue cross-border regulatory harmonization to prevent cybersecurity requirements from impeding digital trade flows. Where feasible, regulators should work to harmonize not only regulations and rules, but also assessments and audits of regulated entities. ONCD, in coordination with the Office of Management and Budget (OMB), will lead the Administration's efforts on cybersecurity regulatory harmonization. The Cyber Incident Reporting Council will coordinate, deconflict, and harmonize Federal incident reporting requirements.

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. In seeking new regulatory authority, the Administration will work with Congress to develop regulatory frameworks that take into account the resources necessary to implement them.

Strategic Objective 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. Combining organizational collaboration and technology-enabled connectivity will create a trust-based "network of networks" that builds situational awareness and drives collective and synchronized action among the cyber defenders that protect our critical infrastructure.

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. In turn, 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 continue to enhance coordination between CISA and other SRMAs, invest in the development of SRMA capabilities, and otherwise enable SRMAs to proactively respond to the needs of critical infrastructure owners and operators in their sectors. The Federal Government will collaborate with industry to define sector-by-sector needs and assess gaps in current SRMA capabilities. Investment by the Federal Government in building out the capabilities of SRMAs will enable security and resilience improvements across critical infrastructure. SRMAs will coordinate with CISA to improve their ability to be proactive and responsive to the needs of their sectors. SRMAs must also continue to support the maturation of third-party collaboration mechanisms. Building on decades of experience collaborating with ISACs and ISAOs, the Federal Government will work with these and other groups to develop a shared vision of how this model should evolve.

Accelerating operational collaboration will require the use of technology solutions to share information and coordinate defensive efforts. 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. In partnership with the private sector, CISA and SRMAs will explore technical and organizational mechanisms to enhance and evolve machine-to-machine sharing of data. The Federal Government will also deepen operational and strategic collaboration with software, hardware, and managed service providers with the capability to reshape the cyber landscape in favor of greater security and resilience.

Strategic Objective 1.3: Integrate Federal Cybersecurity Centers

The Federal Government must coordinate the authorities and capabilities of the departments and agencies that are collectively responsible for supporting the defense of critical infrastructure. Federal Cybersecurity Centers serve as collaborative nodes that fuse together whole-of-government capabilities across the 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.

The Administration has made progress toward this goal, establishing the Joint Cyber Defense Collaborative (JCDC) at CISA to integrate cyber defense planning and operations across the Federal Government and with the private sector and international partners; strengthening the capabilities of the National Cyber Investigative Joint Task Force (NCIJTF) to coordinate law enforcement and other disruption actions; and revitalizing the Cyber Threat Intelligence Integration Center's (CTIIC) role in coordinating intelligence collection, analysis, and partnerships.

Operational collaboration models at SRMAs, such as the Department of Energy (DOE)'s Energy Threat Analysis Center (ETAC) pilot, DoD's Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and the National Security Agency (NSA)'s Cybersecurity Collaboration Center provide opportunities to enable timely, actionable, and relevant information sharing directly with private sector partners in their respective sectors.

Further efforts will be required to strengthen and integrate the Federal Government's operational capabilities and improve integration of the Federal Cybersecurity Centers. ONCD will lead the Administration's efforts to enhance the integration of centers such as these, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale.

Strategic Objective 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. Organizations targeted by cyber threats must know which government agencies to contact for what purposes. The Federal Government must provide clear guidance on how private sector partners can reach Federal agencies for support during cyber incidents and what forms of support the Federal Government may provide.

Consistent with Presidential Policy Directive 41, "United States Cyber Incident Coordination,"—which defines lead roles for the Department of Justice (DOJ), Department of Homeland Security (DHS), and the Office of the Director of National Intelligence in threat, asset, and intelligence

response efforts, respectively—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 the policy that "a call to one is a call to all." When any Federal agency receives a request for assistance, the agency will know what support the wider Federal Government can provide, how to contact the right Federal agencies that can provide such support, and have access to effective information sharing mechanisms. Because most Federal responses take place through field offices, the NCIRP will bolster coordination at the local level, taking lessons from the successes of the Joint Terrorism Task Forces.

When incidents do occur, the 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. These timely notifications and CISA's rapid sharing of relevant information with DOJ and other incident response stakeholders will strengthen our collective defense, improve efforts to identify the root causes of incidents, and inform decision-making within government on how to respond. CISA will consult with SRMAs, DOJ, and other Federal agencies during the CIRCIA rule-making and implementation process to integrate incident reporting systems and ensure real-time sharing and actioning of all relevant incident information.

Following major incidents, we will ensure that the cybersecurity community benefits from lessons learned through the Cyber Safety Review Board (CSRB). Established by EO 14028, "Improving the Nation's Cybersecurity," the CSRB brings together public and private sector cybersecurity leaders to review major cyber incidents, conduct authoritative fact-finding, generate insights that will inform and guide industry remediations, and provide recommendations for improving the nation's cybersecurity posture going forward. 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 1.5: Modernize Federal Defenses

The Federal Government requires secure and resilient information, communications, and operational technology and services to perform its duties. In its first months, this Administration set a new strategic direction for Federal cybersecurity, publishing EO 14028, "Improving the Nation's Cybersecurity," which led to the release of NSM 8, "Improving the Cybersecurity of National Security, the Defense Department, and Intelligence Community Systems," and the OMB Federal zero trust architecture strategy.

Building on this momentum, the Administration will drive long-term efforts to defend the Federal enterprise and modernize Federal systems in accordance with zero trust principles that acknowledge threats must be countered both inside and outside traditional network boundaries. By making its

own networks more defensible and resilient, the Federal Government will be a model for private sector emulation.

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 must continue to build a model for Federal cybersecurity that balances the individual authorities and capabilities of agencies with the security benefits achieved through a collective approach to defense.

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. The software supply chain risk mitigation objective, developed in coordination with NIST, will build on the implementation of EO 14028, "Improving the Nation's Cybersecurity," including the Software Bills of Material (SBOM) efforts, NIST's Secure Software Development Framework, and related efforts to improve open-source software security.

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. These and other cybersecurity goals cannot be achieved unless Federal IT and OT systems are modernized so they are capable of leveraging critical security technologies. 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. The plan will identify milestones to remove all legacy systems incapable of implementing our zero trust architecture strategy within a decade, or otherwise mitigate risks to those that cannot be replaced in that timeframe. 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 TWO | 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. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

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. The Federal Government has increased its capacity to respond to cyber incidents; arrested and successfully prosecuted transnational cybercriminals and state-sponsored actors; imposed sanctions on malicious cyber actors, including bans on travel and denying access to money service providers; and deprived threat actors of access to digital infrastructure and victim networks. The Federal Government has also targeted financial infrastructure used for illicit activity; established new diplomatic initiatives attributing disruptive, destructive, or otherwise destabilizing cyber activities to hold actors accountable for their malicious behavior; and recovered billions of dollars' worth of ill-gotten assets.

We will build upon these successes to enable more sustained and effective disruption of adversaries. 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 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. DOJ and other Federal law enforcement agencies have pioneered the integrated deployment of domestic legal authorities with private industry and international allies and partners to disrupt online criminal infrastructure and resources, from taking down notorious botnets to seizing cryptocurrency gleaned from ransomware and fraud campaigns. Information generated from these investigations enables other efforts, such as victim notification, issuance of cybersecurity advisories, private-sector actions, sanctions designations, diplomatic actions, and intelligence operations.

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. Informed by lessons learned and the rapidly-evolving threat environment, 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.

To increase the volume and speed of these integrated disruption campaigns, the Federal Government must further develop technological and organizational platforms that enable continuous, coordinated operations. 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. Similarly, DoD and the Intelligence Community are committed to bringing to bear their full range of complementary authorities to disruption campaigns.

Strategic Objective 2.2: Enhance Public-Private Operational Collaboration to Disrupt Adversaries

The private sector has growing visibility into adversary activity. This body of insight is often broader and more detailed than that of the Federal Government, due in part to the sheer scale of the private sector and its threat hunting operations, but also due to the rapid pace of innovation in tooling and capabilities. 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. Given the interest of the cybersecurity community and digital infrastructure owners and operators in continuing this approach, we must sustain and expand upon this model so that collaborative disruption operations can be carried out on a continuous basis.

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). Threat-specific collaboration should take the form of nimble, temporary cells, comprised of a small number of trusted operators, hosted and supported by a relevant hub. Using virtual collaboration platforms, members of the cell would share information bidirectionally and work rapidly to disrupt adversaries. The Federal Government will rapidly overcome barriers to supporting and leveraging this collaboration model, such as security requirements and records management policy.

Strategic Objective 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. For instance, the NSA Cybersecurity Collaboration Center's national intelligence-driven engagement with industry has been highly effective at disrupting adversary activity targeting the Defense Industrial Base. Similarly, CISA enables persistent, multi-directional threat information sharing with the private sector through the JCDC and, in coordination with the FBI, uses that information to accelerate victim notification and to reduce the impact of identified intrusions.

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. These processes must provide mechanisms for the private sector to provide timely feedback and their own threat intelligence to the Federal Government to improve targeting of cyber threats for disruption and further intelligence collection. 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 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. Often, these services are leased through foreign resellers who have multiple degrees of separation from their U.S.-based providers, hindering the ability of those providers to address abuse complaints or respond to legal process from U.S. authorities. 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." Implementation of this order will make it more difficult for adversaries to abuse U.S.-based infrastructure while safeguarding individual privacy.

Strategic Objective 2.5: Counter Cybercrime, Defeat Ransomware

Ransomware is a threat to national security, public safety, and economic prosperity. Ransomware operators have disrupted hospitals, schools, pipeline operations, government services, and other critical infrastructure and essential services. Operating from safe havens like Russia, Iran, and North Korea, ransomware actors exploit poor cybersecurity practices to take control of victim networks and rely on cryptocurrencies to receive extortion payments and launder their proceeds.

Given ransomware's impact on key critical infrastructure services, the United States will employ all elements of national power to counter the threat along four lines of effort: (1) leveraging international cooperation to disrupt the ransomware ecosystem and isolate those countries that provide safe havens for criminals; (2) investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors; (3) bolstering critical infrastructure resilience to withstand ransomware attacks; and (4) addressing the abuse of virtual currency to launder ransom payments.

As ransomware is a borderless challenge requiring international cooperation, the White House has convened the Counter-Ransomware Initiative (CRI) with participation from more than thirty countries. The CRI has conducted global exercises to build resilience and, as of January 2023, launched an international counter ransomware task force, led by Australia, to share information regarding the actors and infrastructure conducting ransomware attacks that will support and further accelerate CRI member countries' existing, often coordinated disruption efforts. The CRI will also drive synchronization of policy and diplomatic efforts across its members.

The Administration is committed to mounting disruption campaigns and other efforts that are so sustained, coordinated, and targeted that they render ransomware no longer profitable. 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 United States subjects financial institutions offering covered services in

cryptocurrencies to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls, and the Department of the Treasury, the Secret Service, DOJ, the FBI, and private sector partners are collaborating to trace and interdict ransomware payments. The CRI has gained the commitment of members to implement international AML/CFT standards, including know-your-customer (KYC) rules, to make it harder for ransomware actors to launder cryptocurrency proceeds from attacks. Over the long term, the United States will support implementation of international AML/CFT standards globally to mitigate the use of cryptocurrencies for illicit activities that undermine our national interest as part of our efforts to implement EO 14067, "Ensuring Responsible Development of Digital Assets."

Ultimately, 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. These reports enhance the Federal Government's ability to provide victim support, to prevent further use of cryptocurrencies to evade AML/CFT controls, and to reduce the likelihood that future ransomware attacks will be successful.

PILLAR THREE | SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE

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. We will shift the consequences of poor cybersecurity away from the most vulnerable, making our digital ecosystem more worthy of trust. In this effort, we will not replace or diminish the role of the market, but channel market forces productively toward keeping our country resilient and secure. 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. In too many cases, organizations that choose not to invest in cybersecurity negatively and unfairly impact those that do, often disproportionately impacting small businesses and our most vulnerable communities. While market forces remain the first, best route to agile and effective innovation, they have not adequately mobilized industry to prioritize our core economic and national security interests.

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. We will use Federal purchasing power and grant-making to incentivize security. And we will explore how the government can stabilize insurance markets against catastrophic risk to drive better cybersecurity practices and to provide market certainty when catastrophic events do occur.

Strategic Objective 3.1: Hold the Stewards of Our Data Accountable

Securing personal data is a foundational aspect to protecting consumer privacy in a digital future. Data-driven technologies have transformed our economy and offer convenience for consumers. But the dramatic proliferation of personal information expands the threat environment and increases the impact of data breaches on consumers. When organizations that have data on individuals fail to act as responsible stewards for this data, they externalize the costs onto everyday Americans. Often, the greatest harm falls upon the vulnerable populations for whom risks to their personal data can produce disproportionate harms.

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. By providing privacy requirements that evolve with threats, the United States can pave the way for a more secure future.

Strategic Objective 3.2: Drive the Development of Secure IoT Devices

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. However, 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. Recent IoT vulnerabilities have shown just how easily bad actors can exploit these devices to construct botnets and conduct surveillance.

The Administration will continue to improve IoT cybersecurity through Federal research and development (R&D), procurement, and risk management efforts, as directed in the IoT Cybersecurity Improvement Act of 2020. In addition, the Administration will continue to advance the development of IoT security labeling programs, as directed under EO 14028, "Improving the Nation's Cybersecurity." Through the expansion of IoT security labels, consumers will be able to compare the cybersecurity protections offered by different IoT products, thus creating a market incentive for greater security across the entire IoT ecosystem.

Strategic Objective 3.3: Shift Liability for Insecure Software Products and Services

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. Poor software security greatly increases systemic risk across the digital ecosystem and leave American citizens bearing the ultimate cost.

We must begin to shift liability onto those entities that fail to take reasonable precautions to secure their software while recognizing that even the most advanced software security programs cannot

prevent all vulnerabilities. Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product. Doing so will drive the market to produce safer products and services while preserving innovation and the ability of startups and other small- and medium-sized businesses to compete against market leaders.

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. To begin to shape standards of care for secure software development, 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. This safe harbor will draw from current best practices for secure software development, such as the NIST Secure Software Development Framework. It also must evolve over time, incorporating new tools for secure software development, software transparency, and vulnerability discovery.

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. In partnership with the private sector and the open-source software community, the Federal Government will also continue to invest in the development of secure software, including memory-safe languages and software development techniques, frameworks, and testing tools.

Strategic Objective 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. Through programs funded by the Bipartisan Infrastructure Law, the Inflation Reduction Act, and the CHIPS and Science Act, the United States is making once-in-a-generation investments in our infrastructure and the digital ecosystem that supports it. This Administration is committed to making investments in a manner that increases our collective systemic resilience.

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. Together, we can drive investment in critical products and services that are secure- and resilient-by-design, and sustain and incentivize security and resilience throughout the lifecycle of

critical infrastructure. The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience. And, the Administration will work with Congress to develop other incentive mechanisms to drive better cybersecurity practices at scale.

Strategic Objective 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. EO 14028, "Improving the Nation's Cybersecurity," expands upon this approach, ensuring that contract requirements for cybersecurity are strengthened and standardized across Federal agencies. Continuing to pilot new concepts for setting, enforcing, and testing cybersecurity requirements through procurement can lead to novel and scalable approaches.

When companies make contractual commitments to follow cybersecurity best practices to the Federal Government, they must live up to them. 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.

Strategic Objective 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. In the event of a catastrophic cyber incident, the Federal Government could be called upon to stabilize the economy and aid recovery. Structuring that response before a catastrophic event occurs—rather than rushing to develop an aid package after the fact—could provide certainty to markets and make the nation more resilient. 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. In developing this assessment, the Administration will seek input from, and consult with, Congress, state regulators, and industry stakeholders.

PILLAR FOUR | INVEST IN A RESILIENT FUTURE

A resilient and flourishing digital future tomorrow begins with investments made today. We can build a more secure, resilient, privacy-preserving, and equitable digital ecosystem through strategic investments and coordinated, collaborative action. In doing so, the United States will maintain its leading role as the world's foremost innovator in secure and resilient next-generation technologies and infrastructure.

Foundational elements of our digital ecosystem, like the Internet, are products of sustained and mutually-supporting investments by both public and private sector entities. However, public and private investments in cybersecurity have long trailed the threats and challenges we face. As we build a new generation of digital infrastructure, from next-generation telecommunications and IoT to distributed energy resources, and prepare for revolutionary changes in our technology landscape brought by artificial intelligence and quantum computing, the need to address this investment gap has grown more urgent.

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. We will leverage the National Science Foundation's (NSF) Regional Innovation Engines program, long-standing Secure and Trustworthy Cyberspace program; new grant programs and funding opportunities established in the Bipartisan Infrastructure Law, Inflation Reduction Act, and CHIPS and Science Act; Manufacturing Institutes; and other elements of the Federal research and development enterprise.

These investments will assure continued U.S. leadership in technology and innovation as part of a modern industrial and innovation strategy. 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 complement our efforts to out-innovate other countries with focused, coordinated action to optimize critical and emerging technologies for cybersecurity as they are developed and deployed. 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 4.1: SECURE THE TECHNICAL FOUNDATION 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. The Federal Government will lead by ensuring that its networks have implemented these and other security measures while partnering with stakeholders to develop and drive adoption of solutions that will improve the security of the Internet ecosystem and support research to understand and address reasons for slow adoption.

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 multistakeholder 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. By supporting non-governmental Standards Developing Organizations (SDOs), the United States will partner with industry leaders, international allies, academic institutions, professional societies, consumer groups, and nonprofits, to secure emerging technologies, enable interoperability, foster global market competition, and protect our national security and economic advantage.

Strategic Objective 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.

As part of the update to the Federal Cybersecurity Research and Development Strategic Plan, 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 efforts will be supported by the Federal RD&D enterprise, including the NSF, DOE National Laboratories, and other Federally funded research and development centers (FFRDCs), and through partnerships with academia, manufacturers, technology companies, and owners and operators.

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. This effort will facilitate the proactive identification of potential vulnerabilities, as well as the research to mitigate them. It will also support a larger modern industrial and innovation strategy to promote coordinated and strategic innovation and create markets for trustworthy products and services by comprehensively leveraging Federal investment vehicles, Federal purchasing power, and Federal regulations.

Strategic Objective 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. But quantum computing has the potential to break some of the most ubiquitous encryption standards deployed today. We must prioritize and accelerate investments in widespread replacement of hardware, software, and services that can be easily compromised by quantum computers so that information is protected against future attacks.

To balance the promotion and advancement of quantum computing against threats posed to digital systems, NSM 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes a process for the timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography. 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. The private sector should follow the government's model in preparing its own networks and systems for our post-quantum future.

Strategic Objective 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.

As the United States makes a generational investment in new energy infrastructure, 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. The Administration is coordinating the work of stakeholders across the Federal Government, industry, and SLTT to deploy a secure, interoperable network of electric vehicle chargers, zero-emission fueling infrastructure, and zero-emission transit and school buses. DOE, through efforts such as the Clean Energy Cybersecurity Accelerator (CECA) and the Bipartisan Infrastructure Law-directed Energy Cyber Sense program, and the National Labs are leading the government's effort to secure the clean energy grid of the future and generating security best practices that extend to other critical infrastructure sectors. 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.

Strategic Objective 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. These solutions can support easier and more secure access to government benefits and services, trusted communication and social networks, and new possibilities for digital contracts and payment systems.

Today, the lack of secure, privacy-preserving, consent-based digital identity solutions allows fraud to flourish, perpetuates exclusion and inequity, and adds inefficiency to our financial activities and daily life. Identity theft is on the rise, with data breaches impacting nearly 300 million victims in 2021 and malicious actors fraudulently obtaining billions of dollars in COVID-19 pandemic relief funds intended for small businesses and individuals in need. This malicious activity affects us all, creating significant losses for businesses and producing harmful impacts on public benefit programs and those Americans who use them. Operating independently, neither the private nor public sectors have been able to solve this problem.

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. Building on the NIST-led digital identity research program authorized in the CHIPS and Science Act, these efforts will include strengthening the security of digital credentials; providing attribute and credential validation services; conducting foundational research; updating standards, guidelines, and governance processes to support consistent use and interoperability; and develop digital identity platforms that promote transparency and measurement. Acknowledging that States are piloting mobile drivers' licenses, we note and encourage a focus on privacy, security, civil liberties, equity, accessibility, and interoperability.

In developing these capabilities, our digital identity policies and technologies will protect and enhance individual privacy, civil rights, and civil liberties; guard against unintended consequences, bias, and potential abuse; enable vendor choice and voluntary use by individuals; increase security and interoperability; promote inclusivity and accessibility; and improve transparency and accountability in the use of technology and individuals' data.

Strategic Objective 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. Both private sector and public sector employers face challenges in recruiting, hiring, and retaining professionals to fill these vacancies, which negatively impacts our collective cybersecurity. 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. And, 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. Employers are hiring from too small a pool of talent and from professional networks that and are not able to draw from the full diversity of the country. Women, people of color, first-generation professionals and immigrants, individuals with disabilities, and LGBTQI+ individuals are among the communities which are underrepresented in the field. 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 FIVE | 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.

For decades, we have worked through international institutions to define and advance responsible state behavior in cyberspace. We have used multilateral processes such as the United Nations (UN) Group of Governmental Experts and Open-Ended Working Group to develop a framework that includes a set of peacetime norms and confidence-building measures, which all UN member states have affirmed in the UN General Assembly. We have supported the expansion of the Budapest Convention on Cybercrime and other global efforts to make cyberspace more secure. We will continue these efforts while recognizing the need to work with partners to thwart the dark vision for the future of the Internet that the PRC and other autocratic governments promote. We will do so by demonstrating to economies and societies the value of openness and jointly imposing consequences for behavior that runs counter to agreed norms of state behavior.

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 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 the DFI, the Freedom Online Coalition, and other partnerships and mechanisms, the United States is rallying like-minded countries, the international business community, and other stakeholders to advance our vision for the future of the Internet that

promotes secure and trusted data flows, respects privacy, promotes human rights, and enables progress on broader challenges.

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. The Indo-Pacific Economic Framework for Prosperity (IPEF) and the Americas Partnership for Economic Prosperity (APEP) create opportunities for the United States and regional governments to collaborate in setting rules of the road for the digital economy, including facilitating the development of technical standards, mechanisms to enable cross-border data flows that protect privacy while avoiding strict data localization requirements, and actions to foster supply chain security and resilience. Through the U.S.-EU Trade and Technology Council (TTC), we are coordinating across the Atlantic to combat shared threats and demonstrate how market approaches to digital trade, technology, and innovation can improve the lives of our citizens and be a force for greater prosperity. The United States is also working closely with Australia and the United Kingdom through the trilateral security and technology pact ("AUKUS") to secure critical technologies, improve cyber coordination, and share advanced capabilities.

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. Furthermore, multistakeholder partnerships and coalitions that also include private sector and civil society organizations, such as the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online, the Freedom Online Coalition, and the Global Partnership for Action on Gender-Based Online Harassment and Abuse, are crucial to tackling systemic issues. We will leverage these partnerships to enable effective operational collaboration to defend our shared digital ecosystem. We will also support and help build, as needed, new and innovative partnerships—as in the case of the international Counter-Ransomware Initiative—that bring together unique collections of stakeholders to address new and emerging cybersecurity challenges.

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. The United States will work with its allies and partners to develop new collaborative law enforcement mechanisms for the digital age. For example, the European Cybercrime Centre has played a vital role in modernizing legal frameworks, training law enforcement, improving attribution, collaborating with private sector partners, and responding to malicious cyber activities in Europe. To extend this model, we will support efforts to build effective hubs with partners in other regions.

Strategic Objective 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. Within the law enforcement community, 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. The 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 5.3: Expand U.S. Ability to Assist Allies and Partners

As recent cyberattacks against Costa Rica, Albania, and Montenegro have demonstrated, 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. As one example, the United States is leading a North Atlantic Treaty Organization (NATO) effort to build a virtual cyber incident

support capability that enables Allies to more effectively and efficiently support each other in response to significant malicious cyber activities.

Strategic Objective 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. Increasingly, a community of nations has collaborated to produce coordinated statements of attribution that carry the simultaneous diplomatic condemnation of many governments and strengthening the coalition committed to a stable cyberspace.

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. These efforts will require collaborative use of all tools of statecraft, including diplomatic isolation, economic costs, counter-cyber and law enforcement operations, or legal sanctions, among others.

Strategic Objective 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. Building on the National Strategy to Secure 5G, we are working with our partners to develop secure, reliable, and trustworthy supply chains for 5G and next-generation

wireless networks including through Open Radio Access Networks (Open RAN) and collaborative initiatives to diversify suppliers. Such efforts include DoD testing of Open RAN implementations across multiple bases, with multi-million dollar smart warehouse and logistics projects, and National Telecommunications and Information Administration's (NTIA) work to catalyze the development and adoption of open, interoperable, and standards-based networks through the Public Wireless Supply Chain Innovation Fund. Extending this model to other critical technologies will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more secure, resilient, and trustworthy. The Bipartisan Infrastructure Law mandates "Build America, Buy America" for Federally-funded projects, including for digital infrastructure. Through EO 14017, "America's Supply Chains," the CHIPS and Science Act, and the Inflation Reduction Act, the Federal Government has introduced new industrial and innovation strategy tools to help restore production of critical goods to the United States and its close partners while securing our information technology and advanced manufacturing supply chains.

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. This effort will prioritize opportunities to provide higher levels of assurance that digital technologies will function as expected and to attract countries to support the shared vision of an open, free, global, interoperable, reliable, and secure Internet. The Department of State will further accelerate these efforts through the new International Technology Security and Innovation Fund to support the creation of secure and diverse supply chains for semiconductors and telecommunications. Finally, through implementation of EO 13873, "Securing the Information and Communications Technology and Services Supply Chain," as well as EO 14034 "Protecting Americans' Sensitive Data From Foreign Adversaries," we will work to prevent unacceptable and undue risks to our national security from information and communications technology and services subject to control or influence from adversarial governments.

IMPLEMENTATION

Realizing the strategic objectives outlined in this strategy will require a strong focus on implementation. Under the oversight of NSC staff and in coordination with OMB, ONCD will coordinate implementation of this strategy. ONCD will work with interagency partners to develop and publish an implementation plan to set out the Federal lines of effort necessary to implement this strategy. Where implementation of this strategy requires review of existing policy or the development of new policy, NSC staff will lead this effort through the process described in NSM-2, "Renewing the National Security Council System."

ASSESSING EFFECTIVENESS

In implementing this strategy, the Federal Government will take a data-driven approach. We will measure investments made, our progress toward implementation, and ultimate outcomes and effectiveness of these efforts. ONCD, in coordination with NSC staff, OMB, and departments and agencies, will assess the effectiveness of this strategy and report annually to the President, the Assistant to the President for National Security Affairs, and Congress on the effectiveness of this strategy, associated policy, and follow-on actions in achieving its goals.

INCORPORATING LESSONS LEARNED

The Federal Government will prioritize capturing lessons learned from cyber incidents and apply those lessons in the implementation of this strategy. The CSRB completed its first review on the Log4j vulnerability in summer 2022, during which the CSRB compiled an authoritative account of what happened, from the discovery of the vulnerability to the progression of the largest-scale cyber incident response in history. The CSRB also provided industry, Federal agencies, and the software development community with clear, actionable recommendations based on what the review discovered, so that the community can be better protected going forward.

When the CSRB concludes its reviews, the Federal Government will address its recommendations by improving its own operations through executive action where possible, and will work with Congress to enhance authorities, as necessary. Federal agencies also will promote and amplify CSRB recommendations that are directed to network defenders in the private sector. Beyond the CSRB, a broader national effort to learn from cyber incidents is required. Regulators are encouraged to build incident review processes into their regulatory 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 Federal Government, 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 investment will be required. To guide this investment, ONCD and OMB will jointly issue annual guidance on cybersecurity budget priorities to departments and agencies to further the Administration's strategic approach. 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 change inherent within the cyber ecosystem.