NATIONAL CYBER STRATEGY

of the United States of America

SEPTEMBER 2018



THE WHITE HOUSE

WASHINGTON, DC

My fellow Americans:

Protecting America's national security and promoting the prosperity of the American people are my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities. America created the Internet and shared it with the world. Now, we must make sure to secure and preserve cyberspace for future generations.

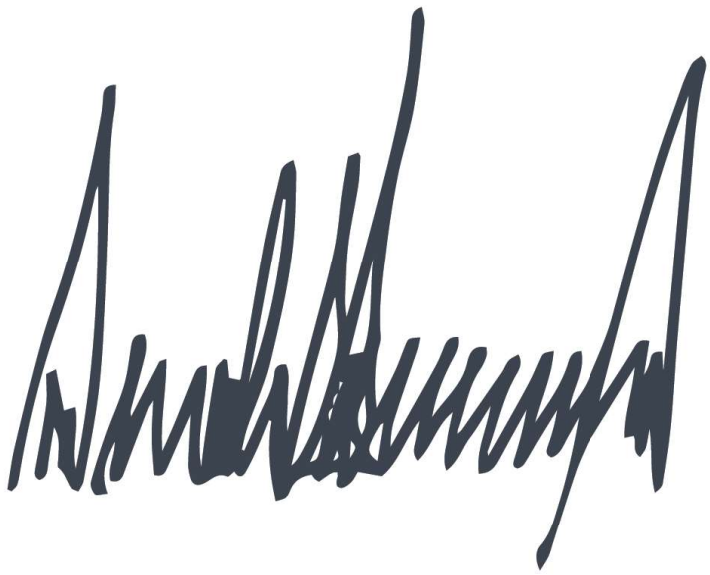
In the last 18 months, my Administration has taken action to address cyber threats. We have sanctioned malign cyber actors. We have indicted those that committed cybercrimes. We have publicly attributed malicious activity to the adversaries responsible and released details about the tools they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing cybersecurity risks to the systems they control, while empowering them to provide adequate security. In addition, last year, I signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The work performed and reports created in response to that Executive Order laid the groundwork for this National Cyber Strategy.

With the release of this National Cyber Strategy, the United States now has its first fully articulated cyber strategy in 15 years. This strategy explains how my Administration will:

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

The National Cyber Strategy demonstrates my commitment to strengthening America's cybersecurity capabilities and securing America from cyber threats. It is a call to action for all Americans and our great companies to take the necessary steps to enhance our national cybersecurity. We will continue to lead the world in securing a prosperous cyber future.

Sincerely,



President Donald J. Trump

The White House
September 2018

Table of Contents

Introduction 1

How Did We Get Here? 1

The Way Forward 2

Pillar I: *Protect the American People, the Homeland, and the American Way of Life* 6

Secure Federal Networks and Information 6

Further Centralize Management and Oversight of Federal Civilian Cybersecurity 6

Align Risk Management and Information Technology Activities 7

Improve Federal Supply Chain Risk Management 7

Strengthen Federal Contractor Cybersecurity 7

Ensure the Government Leads in Best and Innovative Practices 8

Secure Critical Infrastructure 8

Refine Roles and Responsibilities 8

Prioritize Actions According to Identified National Risks 8

Leverage Information and Communications Technology Providers as Cybersecurity Enablers 9

Protect our Democracy 9

Incentivize Cybersecurity Investments 9

Prioritize National Research and Development Investments 9

Improve Transportation and Maritime Cybersecurity 9

Improve Space Cybersecurity 10

Combat Cybercrime and Improve Incident Reporting 10

Improve Incident Reporting and Response 10

Modernize Electronic Surveillance and Computer Crime Laws 11

Reduce Threats from Transnational Criminal Organizations in Cyberspace 11

Improve Apprehension of Criminals Located Abroad 11

Strengthen Partner Nations' Law Enforcement Capacity to Combat Criminal Cyber Activity 11

Pillar II: *Promote American Prosperity* 14

Foster a Vibrant and Resilient Digital Economy 14

Incentivize an Adaptable and Secure Technology Marketplace 14

Prioritize Innovation 14

Invest in Next Generation Infrastructure 15

Promote the Free Flow of Data Across Borders 15

Maintain United States Leadership in Emerging Technologies 15

Promote Full-Lifecycle Cybersecurity 15
Foster and Protect United States Ingenuity 16
Update Mechanisms to Review Foreign Investment and Operation in the United States 16
Maintain a Strong and Balanced Intellectual Property Protection System 16
Protect the Confidentiality and Integrity of American Ideas 16
Develop a Superior Cybersecurity Workforce 17
Build and Sustain the Talent Pipeline 17
Expand Re-Skilling and Educational Opportunities for America's Workers 17
Enhance the Federal Cybersecurity Workforce 17
Use Executive Authority to Highlight and Reward Talent 17

Pillar III: *Preserve Peace through Strength* 20
Enhance Cyber Stability through Norms of Responsible State Behavior 20
Encourage Universal Adherence to Cyber Norms 20
Attribute and Deter Unacceptable Behavior in Cyberspace 21
Lead with Objective, Collaborative Intelligence 21
Impose Consequences 21
Build a Cyber Deterrence Initiative 21
Counter Malign Cyber Influence and Information Operations 21

Pillar IV: *Advance American Influence* 24
Promote an Open, Interoperable, Reliable, and Secure Internet 24
Protect and Promote Internet Freedom 24
Work with Like-Minded Countries, Industry, Academia, and Civil Society 25
Promote a Multi-Stakeholder Model of Internet Governance 25
Promote Interoperable and Reliable Communications Infrastructure and Internet Connectivity 25
Promote and Maintain Markets for United States Ingenuity Worldwide 25
Build International Cyber Capacity 26
Enhance Cyber Capacity Building Efforts 26

Introduction

America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected information technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge. Building on the National Security Strategy and the Administration's progress over its first 18 months, the National Cyber Strategy outlines how the United States will ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity.

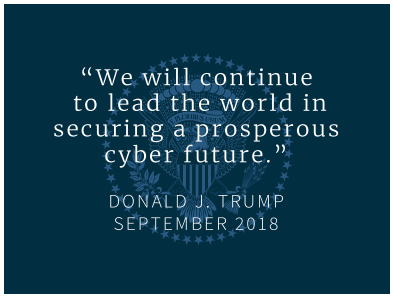
How Did We Get Here?

The rise of the Internet and the growing centrality of cyberspace to all facets of the modern world corresponded with the rise of the United States as the world's lone superpower. For the past quarter century, the ingenuity of the American people drove the evolution of cyberspace, and in turn, cyberspace has become fundamental to American wealth creation and innovation. Cyberspace is an inseparable component of America's financial, social, government, and political life. Meanwhile, Americans sometimes took for granted that the supremacy of the United States in the cyber domain would remain unchallenged, and that America's vision for an open, interoperable, reliable, and secure Internet would inevitably become a reality. Americans believed the growth of the Internet would carry the universal aspirations for free expression and individual liberty around the world. Americans assumed the opportunities to expand communication, commerce, and free exchange of ideas would be self-evident. Large parts of the world have embraced America's vision of a shared and open cyberspace for the mutual benefit of all.

Our competitors and adversaries, however, have taken an opposite approach. They benefit from the open Internet, while constricting and controlling their own people's access to it, and actively undermine the principles of an open Internet in international forums. They hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world. They view cyberspace as an arena where the United States' overwhelming military, economic, and political power could be neutralized and where the United States and its allies and partners are vulnerable.

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and inter-

national businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft. Non-state actors — including terrorists and criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states. Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities. Entities across the United States have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data as well as detecting, responding to, and recovering from incidents.



The Way Forward

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive. Securing cyberspace is fundamental to our strategy and requires technical advancements and administrative efficiency across the Federal Government and the private sector. The Administration also recognizes that a purely technocratic approach to cyberspace is insufficient to address the nature of the new problems we confront. The United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation. The Administration is already taking action to aggressively address these threats and adjust to new realities. The United States has sanctioned malign cyber actors and indicted those that have committed cybercrimes. We have publicly attributed malicious activity to the responsible adversaries and released details of the tools and infrastructure they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing the cybersecurity risks to systems they control, while empowering them to provide adequate security.

The Administration's approach to cyberspace is anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy. We retain our commitment to the promise of an open, interoperable, reliable, and secure Internet to strengthen and extend our values and protect and ensure economic security for American workers and companies. The future we desire will not come without a renewed American commitment to advance our interests across cyberspace.

The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property,

and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons.

This National Cyber Strategy outlines how we will (1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives.

The articulation of the National Cyber Strategy is organized according to the pillars of the National Security Strategy. The National Security Council staff will coordinate with departments, agencies, and the Office of Management and Budget (OMB) on an appropriate resource plan to implement this Strategy. Departments and agencies will execute their missions informed by the following strategic guidance.

PILLAR I

Protect the American People, the Homeland, and the American Way of Life

Protecting the American people, the American way of life, and American interests is at the forefront of the National Security Strategy. Protecting American information networks, whether government or private, is vital to fulfilling this objective. It will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime. The United States Government, private industry, and the public must each take immediate and decisive actions to strengthen cybersecurity, with each working on securing the networks under their control and supporting each other as appropriate.

OBJECTIVE: Manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems.

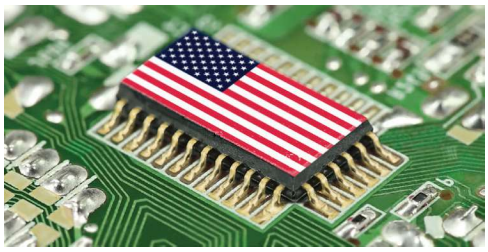
Secure Federal Networks and Information

The responsibility to secure Federal networks — including Federal information systems and national security systems — falls squarely on the Federal Government. The Administration will clarify the relevant authorities, responsibilities, and accountability within and across departments and agencies for securing Federal information systems, while setting the standard for effective cybersecurity risk management. As part of this effort, the Administration will centralize some authorities within the Federal Government, enable greater cross-agency visibility, improve management of our Federal supply chain, and strengthen the security of United States Government contractor systems.

Priority Actions

FURTHER CENTRALIZE MANAGEMENT AND OVERSIGHT OF FEDERAL CIVILIAN CYBERSECURITY: The Administration will act to further enable the Department of Homeland Security (DHS) to secure Federal department and agency networks, with the exception of national security systems and Department of Defense (DOD) and Intelligence Community (IC) systems. This includes ensuring DHS has appropriate access to agency information systems for cybersecurity purposes and can take and direct action to safeguard systems from the spectrum of risks. Under the oversight of the OMB, the Administration will expand on work begun under Executive Order (E.O.) 13800 to prioritize the transition of agencies to shared services

and infrastructure. DHS will have appropriate visibility into those services and infrastructure to improve United States cybersecurity posture. We will continue to deploy centralized capabilities, tools, and services through DHS where appropriate, and improve oversight and compliance with applicable laws, policies, standards, and directives. This will likely require new policies and architectures that enable the government to better leverage innovation. DOD and the IC will consider these activities as they work to better secure national security systems, DOD systems, and IC systems, as appropriate.



ALIGN RISK MANAGEMENT AND INFORMATION TECHNOLOGY ACTIVITIES: E.O. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*, empowers Chief Information Officers (CIOs) to more effectively leverage technology to accomplish agency missions, cut down on duplication, and make information technology (IT) investment more efficient. Department and agency leaders will empower and hold their CIOs accountable to align cybersecurity risk management decisions and IT budgeting and procurement decisions. The Administration, through OMB and DHS, will continue to guide and direct risk management actions across Federal civilian departments and agencies, and CIOs will be empowered to take a proactive leadership role in assuring IT procurement decisions assign the proper priority to securing networks and data.

IMPROVE FEDERAL SUPPLY CHAIN RISK MANAGEMENT: The Administration will integrate supply chain risk management into agency procurement and risk management processes in accordance with federal requirements that are consistent with industry best practices to better ensure the technology that the Federal Government deploys is secure and reliable. This includes ensuring better information sharing among departments and agencies to improve awareness of supply chain threats and reduce duplicative supply chain activities within the United States Government, including by creating a supply chain risk assessment shared service. It also includes addressing deficiencies in the Federal acquisition system, such as providing more streamlined authorities to exclude risky vendors, products, and services when justified. This effort will be synchronized with efforts to manage supply chain risk in the Nation's infrastructure.

STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY: The United States cannot afford to have sensitive government information or systems inadequately secured by contractors. Federal contractors provide important services to the United States Government and must properly secure the systems through which they provide those services. Going forward, the Federal Government will be able to assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, sensoring, and responding to incidents on contractor systems. Contracts with Federal departments and agencies will be drafted to authorize such activities for the purpose of improving cybersecurity. Among the acute concerns in this area are those contractors within the defense industrial base responsible for researching and developing key systems fielded by the DOD. Further, as recommended in the E.O. 13800 *Report to the President on Federal IT Modernization*, the Administration will support

adoption of consolidated acquisition strategies to improve cybersecurity and reduce overhead costs associated with using inconsistent contract provisions across the Federal Government. It will also act to ensure, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information to improve their security posture.

ENSURE THE GOVERNMENT LEADS IN BEST AND INNOVATIVE PRACTICES: The Federal Government will ensure the systems it owns and operates meet the standards and cybersecurity best practices it recommends to industry. Projects that receive Federal funding must meet these standards as well. The Federal Government will use its purchasing power to drive sector-wide improvement in products and services. The Federal Government will also be a leader in developing and implementing standards and best practices in new and emerging areas. For example, public key cryptography is foundational to the secure operation of our infrastructure. To protect against the potential threat of quantum computers being able to break modern public key cryptography, the Department of Commerce, through the National Institute of Standards and Technology (NIST), will continue to solicit, evaluate, and standardize quantum-resistant, public key cryptographic algorithms. The United States must be at the forefront of protecting communications by supporting rapid adoption of these forthcoming NIST standards across government infrastructure and by encouraging the Nation to do the same.

Secure Critical Infrastructure

The responsibility to secure the Nation's critical infrastructure and manage its cybersecurity risk is shared by the private sector and the Federal Government. In partnership with the private sector, we will collectively use a risk-management approach to mitigating vulnerabilities to raise the base level of cybersecurity across critical infrastructure. We will simultaneously use a consequence-driven approach to prioritize actions that reduce the potential that the most advanced adversaries could cause large-scale or long-duration disruptions to critical infrastructure. We will also deter malicious cyber actors by imposing costs on them and their sponsors by leveraging a range of tools, including but not limited to prosecutions and economic sanctions, as part of a broader deterrence strategy.

Priority Actions

REFINE ROLES AND RESPONSIBILITIES: The Administration will clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response. Clarity will enable proactive risk management that comprehensively addresses threats, vulnerabilities, and consequences. It will also identify and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination.

PRIORITIZE ACTIONS ACCORDING TO IDENTIFIED NATIONAL RISKS: The Federal Government will work with the private sector to manage risks to critical infrastructure at the greatest risk. The Administration will develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks. The Administration will prioritize risk-reduction activities across seven key areas: national security, energy and power, banking and

finance, health and safety, communications, information technology, and transportation.

LEVERAGE INFORMATION AND COMMUNICATIONS TECHNOLOGY PROVIDERS AS CYBERSECURITY ENABLERS: Information and communications technology (ICT) underlies every sector in America. ICT providers are in a unique position to detect, prevent, and mitigate risk before it impacts their customers, and the Federal Government must work with these providers to improve ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties. The United States Government will strengthen efforts to share information with ICT providers to enable them to respond to and remediate known malicious cyber activity at the network level. This will include sharing classified threat and vulnerability information with cleared ICT operators and downgrading information to the unclassified level as much as possible. We will promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards. The United States Government will convene stakeholders to devise cross-sector solutions to challenges at the network, device, and gateway layers, and we will encourage industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape.

PROTECT OUR DEMOCRACY: Securing our democratic processes is of paramount importance to the United States and our democratic allies. State and local government officials own and operate diverse election infrastructure within the United States. Therefore, when requested we will provide technical and risk management services, support training and exercising, maintain situational awareness of threats to this sector, and improve the sharing of threat intelligence with those officials to better prepare and protect the election infrastructure. The Federal Government will continue to coordinate the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system. In the event of a significant cyber incident, the Federal Government is poised to provide threat and asset response to recover election infrastructure.

INCENTIVIZE CYBERSECURITY INVESTMENTS: Most cybersecurity risks to critical infrastructure stem from the exploitation of known vulnerabilities. The United States Government will work with private and public sector entities to promote understanding of cybersecurity risk so they make more informed risk-management decisions, invest in appropriate security measures, and realize benefits from those investments.

PRIORITIZE NATIONAL RESEARCH AND DEVELOPMENT INVESTMENTS: The Federal Government will update the National Critical Infrastructure Security and Resilience Research and Development Plan to set priorities for addressing cybersecurity risks to critical infrastructure. Departments and agencies will align their investments to the priorities, which will focus on building new cybersecurity approaches that use emerging technologies, improving information-sharing and risk management related to cross-sector interdependencies, and building resilience to large-scale or long-duration disruptions.

IMPROVE TRANSPORTATION AND MARITIME CYBERSECURITY: America's economic and national security is built on global trade and transportation. Our ability to guarantee free and timely movement of goods, open sea and air lines of communications, access to oil and natural gas, and availability of associated critical infrastructures is vital to our economic and national security. As these sectors have modernized,

they have also become more vulnerable to cyber exploitation or attack. Maritime cybersecurity is of particular concern because lost or delayed shipments can result in strategic economic disruptions and potential spillover effects on downstream industries. Given the criticality of maritime transportation to the United States and global economy and the minimal risk-reduction investments to protect against cyber exploitation made thus far, the United States will move quickly to clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure. The United States will assure the uninterrupted transport of goods in the face of all threats that can hold this inherently international infrastructure at risk through cyber means.

IMPROVE SPACE CYBERSECURITY: The United States considers unfettered access to and freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. The Administration is concerned about the growing cyber-related threats to space assets and supporting infrastructure because these assets are critical to functions such as positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communications; and weather monitoring. The Administration will enhance efforts to protect our space assets and support infrastructure from evolving cyber threats, and we will work with industry and international partners to strengthen the cyber resilience of existing and future space systems.

Combat Cybercrime and Improve Incident Reporting

Federal departments and agencies, in cooperation with state, local, tribal, and territorial government entities, play a critical role in detecting, preventing, disrupting, and investigating cyber threats to our Nation. The United States is regularly the victim of malicious cyber activity perpetrated by criminal actors, including state and non-state actors and their proxies and terrorists using network infrastructure in the United States and abroad. Federal law enforcement works to apprehend and prosecute offenders, disable criminal infrastructure, limit the spread and use of nefarious cyber capabilities, prevent cyber criminals and their state sponsors from profiting from their illicit activity, and seize their assets. The Administration will push to ensure that our Federal departments and agencies have the necessary legal authorities and resources to combat transnational cybercriminal activity, including identifying and dismantling botnets, dark markets, and other infrastructure used to enable cybercrime, and combatting economic espionage. To effectively deter, disrupt, and prevent cyber threats, law enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies, to obtain time-sensitive evidence pursuant to appropriate legal process. Law enforcement actions to combat criminal cyber activity serve as an instrument of national power by, among other things, deterring those activities.

Priority Actions

IMPROVE INCIDENT REPORTING AND RESPONSE: The United States Government will continue to encourage reporting of intrusions and theft of data by all victims, especially critical infrastructure partners. The prompt reporting of cyber incidents to the Federal Government is essential to an effective response, linking of

related incidents, identification of the perpetrators, and prevention of future incidents.

MODERNIZE ELECTRONIC SURVEILLANCE AND COMPUTER CRIME LAWS: The Administration will work with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors.

REDUCE THREATS FROM TRANSNATIONAL CRIMINAL ORGANIZATIONS IN CYBERSPACE: Computer hacking conducted by transnational criminal groups poses a significant threat to our national security. Equipped with sizeable funds, organized criminal groups operating abroad employ sophisticated malicious software, spear-phishing campaigns, and other hacking tools — some of which rival those of nation states in sophistication — to hack into sensitive financial systems, conduct massive data breaches, spread ransomware, attack critical infrastructure, and steal intellectual property. The Administration will advocate for law enforcement to have effective legal tools to investigate and prosecute such groups and modernized organized crime statutes for use against this threat.

IMPROVE APPREHENSION OF CRIMINALS LOCATED ABROAD: Deterring cybercrime requires a credible threat that perpetrators will be identified, apprehended, and brought to justice. However, some foreign nations choose not to cooperate with extradition requests, impose unreasonable limitations, or actively interfere in these efforts. The United States will continue to identify gaps and potential mechanisms for bringing foreign-based cyber criminals to justice. The United States Government will also increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests. We will push other nations to expedite their assistance in investigations and to comply with any bilateral or multilateral agreements or obligations.

STRENGTHEN PARTNER NATIONS' LAW ENFORCEMENT CAPACITY TO COMBAT CRIMINAL CYBER ACTIVITY: The United States should also aid willing partner nations to build their capacity to address criminal cyber activity. The borderless nature of cybercrime, including state-sponsored and terrorist activities, requires strong international law enforcement partnerships. This cooperation requires foreign law enforcement agencies to have the technical capability to assist United States law enforcement effectively when requested. It is therefore in the interest of United States national security to continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation.

The United States will strive to improve international cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence. The United States will also lead in developing interoperable and mutually beneficial systems to encourage efficient cross-border information exchange for law enforcement purposes and reduce barriers to coordination. The Administration will urge effective use of existing international tools like the United Nations Convention Against Transnational Organized Crime and the G7 24/7 Network Points of Contact. Finally, we will work to expand the international consensus favoring the Convention on Cybercrime of the Council of Europe (Budapest Convention), including by supporting greater adoption of the convention.



PILLAR II

Promote American Prosperity

The Internet has generated tremendous benefits domestically and abroad, and it helps to advance American values of freedom, security, and prosperity. Along with its expansion have come challenges that threaten our national security. The United States will demonstrate a coherent and comprehensive approach to address these and other challenges to defend American national interests in this increasingly digitized world.

OBJECTIVE: Preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency.

Foster a Vibrant and Resilient Digital Economy

Economic security is inherently tied to our national security. As the foundations of our economy are becoming increasingly rooted in digital technologies, the United States Government will model and promote standards that protect our economic security and reinforce the vitality of the American marketplace and American innovation.

Priority Actions

INCENTIVIZE AN ADAPTABLE AND SECURE TECHNOLOGY MARKETPLACE: To enhance the resilience of cyberspace, the Administration expects the technology marketplace to support and reward the continuous development, adoption, and evolution of innovative security technologies and processes. The Administration will work across stakeholder groups, including the private sector and civil society, to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies. The Administration will improve awareness and transparency of cybersecurity practices to build market demand for more secure products and services. Finally, the Administration will collaborate with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges to include platform and managed service approaches that lower barriers to secure practice adoption across the breadth of the ecosystem.

PRIORITIZE INNOVATION: The United States Government will promote implementation and

continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem. These standards and practices should be outcome-oriented and based on sound technological principles rather than point-in-time company specifications. The Administration will eliminate policy barriers that inhibit a robust cybersecurity industry from developing, sharing, and building innovative capabilities to reduce cyber threats.

INVEST IN NEXT GENERATION INFRASTRUCTURE: The Administration will facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure here in the United States, while using the buying power of the Federal Government to incentivize the move towards more secure supply chains. The United States Government will work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements. The United States Government will examine the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application. We will collaborate with the private sector and civil society to understand trends in technology advancement to maintain the United States technological edge in connected technologies and to ensure secure practices are adopted from the outset.

> "The National Cyber Strategy is a call to action for all Americans and our great companies to take the necessary steps to enhance our national cybersecurity."
>
> DONALD J. TRUMP
> SEPTEMBER 2018

PROMOTE THE FREE FLOW OF DATA ACROSS BORDERS: Countries are increasingly looking towards restrictive data localization and regulations as pretexts for digital protectionism under the rubric of national security. Those actions negatively impact the competitiveness of United States companies. The United States will continue to lead by example and push back against unjustifiable barriers to the free flow of data and digital trade. The Administration will continue to work with international counterparts to promote open, industry driven standards, innovative products, and risk-based approaches that permit global innovation and the free flow of data while meeting the legitimate security needs of the United States.

MAINTAIN UNITED STATES LEADERSHIP IN EMERGING TECHNOLOGIES: The United States' influence in cyberspace is linked to our technological leadership. Accordingly, the United States Government will make a concerted effort to protect cutting edge technologies, including from theft by our adversaries, support those technologies' maturation, and, where possible, reduce United States companies' barriers to market entry. The United States will promote United States cybersecurity innovation worldwide through trade-related engagement, raising awareness of innovative American cybersecurity tools and services, exposing and countering repressive regimes use of such tools and services to undermine human rights, and reducing barriers to a robust global cybersecurity market.

PROMOTE FULL-LIFECYCLE CYBERSECURITY: The United States Government will promote full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery. We will identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace, encour-

aging manufacturers to differentiate products based on the quality of their security features. The United States Government will promote foundational engineering practices to reduce systemic fragility and develop designs that degrade and recover effectively when successfully attacked. The United States Government will also promote regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries. This includes promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack. The United States Government will also evaluate how to improve the end-to-end lifecycle for digital identity management, including over-reliance on Social Security numbers.

Foster and Protect United States Ingenuity

Fostering and protecting American invention and innovation is critical to maintaining the United States' strategic advantage in cyberspace. The United States Government will nurture innovation by promoting institutions and programs that drive United States competitiveness. The United States Government will counter predatory mergers and acquisitions and counter intellectual property theft. We will also catalyze United States leadership in emerging technologies and promote government identification and support to these technologies, which include artificial intelligence, quantum information science, and next-generation telecommunication infrastructure.

Priority Actions

UPDATE MECHANISMS TO REVIEW FOREIGN INVESTMENT AND OPERATION IN THE UNITED STATES: The confidentiality, integrity, and availability of United States telecommunications networks are essential to our economy and national security. We must be vigilant to safeguard the telecommunications networks we depend on in our everyday lives so they cannot be used or compromised by a foreign adversary to harm the United States. The United States Government will balance these objectives by formalizing and streamlining the review of Federal Communications Commission referrals for telecommunications licenses. The United States Government will facilitate a transparent process to increase the efficiency of this review.

MAINTAIN A STRONG AND BALANCED INTELLECTUAL PROPERTY PROTECTION SYSTEM: Strong intellectual property protections ensure continued economic growth and innovation in the digital age. The United States Government has fostered and will continue to help foster a global intellectual property rights system that provides incentives for innovation through the protection and enforcement of intellectual property rights such as patents, trademarks, and copyrights. The United States Government will also promote protection of sensitive emerging technologies and trade secrets, and we will work to prevent adversarial nation states from gaining unfair advantage at the expense of American research and development.

PROTECT THE CONFIDENTIALITY AND INTEGRITY OF AMERICAN IDEAS: For more than a decade, malicious actors have conducted cyber intrusions into United States commercial networks, targeting confidential business information held by American firms. Malicious cyber actors from other nations have stolen troves of trade secrets, technical data, and sensitive proprietary internal communications. The United States Government will work against the illicit appro-

priation of public and private sector technology and technical knowledge by foreign competitors, while maintaining an investor-friendly climate.

Develop a Superior Cybersecurity Workforce

A highly skilled cybersecurity workforce is a strategic national security advantage. The United States will fully develop the vast American talent pool, while at the same time attracting the best and brightest among those abroad who share our values.

Priority Actions

BUILD AND SUSTAIN THE TALENT PIPELINE: Our peer competitors are implementing workforce development programs that have the potential to harm long-term United States cybersecurity competitiveness. The United States Government will continue to invest in and enhance programs that build the domestic talent pipeline, from primary through postsecondary education. The Administration will leverage the President's proposed merit-based immigration reforms to ensure that the United States has the most competitive technology sector. This effort may require additional legislation to achieve the sought after goals.

EXPAND RE-SKILLING AND EDUCATIONAL OPPORTUNITIES FOR AMERICA'S WORKERS: The Administration will work with the Congress to promote and reinvigorate educational and training opportunities to develop a robust cybersecurity workforce. This includes expanding Federal recruitment, training, re-skilling people from a broad range of backgrounds, and giving them opportunities to re-train into cybersecurity careers.

ENHANCE THE FEDERAL CYBERSECURITY WORKFORCE: To improve recruitment and retention of highly qualified cybersecurity professionals to the Federal Government, the Administration will continue to use the National Initiative for Cybersecurity Education (NICE) Framework to support policies allowing for a standardized approach for identifying, hiring, developing, and retaining a talented cybersecurity workforce. Additionally, the Administration will explore appropriate options to establish distributed cybersecurity personnel under the management of DHS to oversee the development, management, and deployment of cybersecurity personnel across Federal departments and agencies with the exception of DOD and the IC. The Administration will promote appropriate financial compensation for the United States Government workforce, as well as unique training and operational opportunities to effectively recruit and retain critical cybersecurity talent in light of the competitive private sector environment.

USE EXECUTIVE AUTHORITY TO HIGHLIGHT AND REWARD TALENT: The United States Government will promote and magnify excellence by highlighting cybersecurity educators and cybersecurity professionals. The United States Government will also leverage public-private collaboration to develop and circulate the NICE Framework, which provides a standardized approach for identifying cybersecurity workforce gaps, while also implementing actions to prepare, grow, and sustain a workforce that can defend and bolster America's critical infrastructure and innovation base.

Preserve Peace through Strength

Challenges to United States security and economic interests, from nation states and other groups, which have long existed in the offline world are now increasingly occurring in cyberspace. This now-persistent engagement in cyberspace is already altering the strategic balance of power. This Administration will issue transformative policies that reflect today's new reality and guide the United States Government towards strategic outcomes that protect the American people and our way of life. Cyberspace will no longer be treated as a separate category of policy or activity disjointed from other elements of national power. The United States will integrate the employment of cyber options across every element of national power.

OBJECTIVE: Identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace.

Enhance Cyber Stability through Norms of Responsible State Behavior

The United States will promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity. These principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework.

Priority Action

ENCOURAGE UNIVERSAL ADHERENCE TO CYBER NORMS: International law and voluntary non-binding norms of responsible state behavior in cyberspace provide stabilizing, security-enhancing standards that define acceptable behavior to all states and promote greater predictability and stability in cyberspace. The United States will encourage other nations to publicly affirm these principles and views through enhanced outreach and engagement in multilateral fora. Increased public affirmation by the United States and other governments will lead to accepted expectations of state behavior and thus contribute to greater predictability and stability in cyberspace.

Attribute and Deter Unacceptable Behavior in Cyberspace

As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners. All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities. The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners.

Priority Actions

LEAD WITH OBJECTIVE, COLLABORATIVE INTELLIGENCE: The IC will continue to lead the world in the use of all-source cyber intelligence to drive the identification and attribution of malicious cyber activity that threatens United States national interests. Objective and actionable intelligence will be shared across the United States Government and with key partners to identify hostile foreign nation states, and non-nation state cyber programs, intentions, capabilities, research and development efforts, tactics, and operational activities that will inform whole-of-government responses to protect American interests at home and abroad.

IMPOSE CONSEQUENCES: The United States will develop swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior. The Administration will conduct interagency policy planning for the time periods leading up to, during, and after the imposition of consequences to ensure a timely and consistent process for responding to and deterring malicious cyber activities. The United States will work with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against our nation and interests.

BUILD A CYBER DETERRENCE INITIATIVE: The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states. The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior. The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.

COUNTER MALIGN CYBER INFLUENCE AND INFORMATION OPERATIONS: The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation. This includes working with foreign government partners as well as the private sector, academia, and civil society to identify, counter, and prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties.



PILLAR IV

Advance American Influence

The world looks to the United States, where much of the innovation for today's Internet originated, for leadership on a vast range of transnational cyber issues. The United States will maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace. Collaboration with allies and partners is also essential to ensure we can continue to benefit from the cross-border communications, content creation, and commerce generated by the open, interoperable architecture of the Internet.

OBJECTIVE: Preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests.

Promote an Open, Interoperable, Reliable, and Secure Internet

The global Internet has prompted some of the greatest advancements since the industrial revolution, enabling great advances in commerce, health, communications, and other national infrastructure. At the same time, centuries-old battles over human rights and fundamental freedoms are now playing out online. Freedoms of expression, peaceful assembly, and association, as well as privacy rights, are under threat. Despite unprecedented growth, the Internet's economic and social potential continues to be undermined by online censorship and repression. The United States stands firm on its principles to protect and promote an open, interoperable, reliable, and secure Internet. We will work to ensure that our approach to an open Internet is the international standard. We will also work to prevent authoritarian states that view the open Internet as a political threat from transforming the free and open Internet into an authoritarian web under their control, under the guise of security or countering terrorism.

Priority Actions

PROTECT AND PROMOTE INTERNET FREEDOM: The United States Government conceptualizes Internet freedom as the online exercise of human rights and fundamental freedoms — such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online — regardless of frontiers or medium. By extension, Internet freedom also supports the free

flow of information online that enhances international trade and commerce, fosters innovation, and strengthens both national and international security. As such, United States Internet freedom principles are inextricably linked to our national security. Internet freedom is also a key guiding principle with respect to other United States foreign policy issues, such as cybercrime and counterterrorism efforts. Given its importance, the United States will encourage other countries to advance Internet freedom through venues such as the Freedom Online Coalition, of which the United States is a founding member.

WORK WITH LIKE-MINDED COUNTRIES, INDUSTRY, ACADEMIA, AND CIVIL SOCIETY: The United States will continue to work with like-minded countries, industry, civil society, and other stakeholders to advance human rights and Internet freedom globally and to counter authoritarian efforts to censor and influence Internet development. The United States Government will continue to support civil society through integrated support for technology development, digital safety training, policy advocacy, and research. These programs aim to enhance the ability of individual citizens, activists, human rights defenders, independent journalists, civil society organizations, and marginalized populations to safely access the uncensored Internet and promote Internet freedom at the local, regional, national, and international levels.

PROMOTE A MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE: The United States will continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet. The multi-stakeholder model of Internet governance is characterized by transparent, bottom-up, consensus-driven processes and enables governments, the private sector, civil society, academia, and the technical community to participate on equal footing. The United States Government will defend the open, interoperable nature of the Internet in multilateral and international fora through active engagement in key organizations, such as the Internet Corporation for Assigned Names and Numbers, the Internet Governance Forum, the United Nations, and the International Telecommunication Union.

PROMOTE INTEROPERABLE AND RELIABLE COMMUNICATIONS INFRASTRUCTURE AND INTERNET CONNECTIVITY: The United States will promote communications infrastructure and Internet connectivity that is open, interoperable, reliable, and secure. Such investment will provide greater opportunities for American firms to compete while countering the influence of statist, top-down government interventions in areas of strategic competition. It will also protect America's security and commercial interests by strengthening United States industry's competitive position in the global digital economy. The Administration will also support and promote open, industry-led standards activities based on sound technological principles.

PROMOTE AND MAINTAIN MARKETS FOR UNITED STATES INGENUITY WORLDWIDE: American innovators and security professionals have contributed significantly in designing products and services that improve our ability to communicate and interact globally and that protect communications infrastructure, data, and devices worldwide. The United States will continue to promote markets for American ingenuity overseas, including for emerging technologies that can lower the cost of security. The United States will also advise on infrastructure deploy-

ments, innovation, risk management, policy, and standards to further the global Internet's reach and to ensure interoperability, security, and stability. Finally, the United States will work with international partners, government, industry, civil society, technologists, and academics to improve the adoption and awareness of cybersecurity best practices worldwide.

Build International Cyber Capacity

Capacity building equips partners to protect themselves and assist the United States in addressing threats that target mutual interests, while serving broader diplomatic, economic, and security goals. Through cyber capacity building initiatives, the United States builds strategic partnerships that promote cybersecurity best practices through a common vision of an open, interoperable, reliable, and secure Internet that encourages investment and opens new economic markets. In addition, capacity building allows for additional opportunities to share cyber threat information, enabling the United States Government and our partners to better defend domestic critical infrastructure and global supply chains, as well as focus whole-of-government cyber engagements. Our leadership in building partner cybersecurity capacity is critical to maintaining American influence against global competitors. Building partner cyber capacity will empower international partners to implement policies and practices which allow them to be effective partners in the United States-led Cyber Deterrence Initiative.

Priority Action

ENHANCE CYBER CAPACITY BUILDING EFFORTS: Many United States allies and partners possess unique cyber capabilities that can complement our own. The United States will work to strengthen the capacity and interoperability of those allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats. Partners can also help detect, deter, and defeat those shared threats in cyberspace. In order for international partners to effectively protect their digital infrastructure and combat shared threats, while realizing the economic and social gains derived from the Internet and ICTs, the United States will continue to address the building blocks for organizing national efforts on cybersecurity. We will also aggressively expand efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges. In addition, the United States will work to reduce the impact and influence of transnational cybercrime and terrorist activities by partnering with and strengthening the security and law enforcement capabilities of our partners to build their cyber capacity.

Notes

Notes