US National Cybersecurity Strategy

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy

- Issued March 1, 2023 from the White House - https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* and the work performed and reports created in response to that Executive Order laid the groundwork for this National Cyber Strategy
- This National Cyber Strategy provides the first fully articulated US cyber strategy in 15 years
- This strategy explains how the US 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy Current Landscape

- Rise of the open internet has allowed US competitors and advisories to engage in pernicious economic espionage and malicious cyber activities such as cyber attacks, cyber-enabled economic espionage and trillions of dollars of intellectual property theft , causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world
- 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 US 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy Current Landscape

- A cybersecurity strategy to counteract these malicious cyber activities must recognize that:
  - Purely technocratic approach to cyberspace is insufficient to address the nature of these new problems
  - Must impose costs if it hopes to deter malicious cyber actors and prevent further escalation
  - Must be anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy
  - Must retain 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 US is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks
  - The US is 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy Four Pillars

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

- Will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime

II. Promote American Prosperity

- Need to demonstrate a coherent and comprehensive approach to address challenges that threaten our national security in this increasingly digitized world

III. Preserve Peace through Strength

- Need to issue transformative policies that reflect today's new reality where Cyberspace is no longer treated as a separate category of policy or activity disjointed from other elements of national power

IV. Advance American Influence

- Need to 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

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

Steps

1. Secure Federal Networks and Information by**:**

- **FURTHER CENTRALIZE MANAGEMENT AND OVERSIGHT OF FEDERAL CIVILIAN CYBERSECURITY**
  - 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
  - Expand on work begun under Executive Order (E.O.) 13800 to prioritize the transition of agencies to shared services and infrastructure
  - Deploy centralized capabilities, tools, and services through DHS where appropriate, and improve oversight and compliance with applicable laws, policies, standards, and directives

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

1. **Secure Federal Networks and Information** by**:**
   - **ALIGN RISK MANAGEMENT AND INFORMATION TECHNOLOGY ACTIVITIES**
     - 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 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**
     - Integrate supply chain risk management into agency procurement and risk management processes in accordance with federal requirements that are consistent with industry best practices
     - Ensure, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

1. Secure Federal Networks and Information by**:**

- **STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY**
  - Assess the security of its data by reviewing contractor risk management practices and adequately testing, hunting, censoring, and responding to incidents on contractor systems
  - Support adoption of consolidated acquisition strategies to improve cybersecurity and reduce overhead costs associated with using inconsistent contract provisions across the Federal Government
  - Ensure, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information
- **ENSURE THE GOVERNMENT LEADS IN BEST AND INNOVATIVE PRACTICES**
  - Ensure the systems it owns and operates meet the standards and cybersecurity best practices it recommends to industry
  - Use its purchasing power to drive sector-wide improvement in products and services
  - Be a leader in developing and implementing standards and best practices in new and emerging areas such as quantum computing

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **REFINE ROLES AND RESPONSIBILITIES**
  - Clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response
  - 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**
  - Work with the private sector to manage risks to critical infrastructure at the greatest risk
  - 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
  - Prioritize risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **LEVERAGE INFORMATION AND COMMUNICATIONS TECHNOLOGY PROVIDERS AS CYBERSECURITY ENABLERS**
  - Strengthen efforts to share information with ICT providers to enable them to respond to and remediate known malicious cyber activity at the network level
  - Promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards
  - Encourage industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape
- **PROTECT OUR DEMOCRACY**
  - When requested, 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
  - Coordinate the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **INCENTIVIZE CYBERSECURITY INVESTMENTS**
  - 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**
  - Update the National Critical Infrastructure Security and Resilience Research and Development Plan to set priorities for addressing cybersecurity risks to critical infrastructure
  - Align 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **IMPROVE TRANSPORTATION AND MARITIME CYBERSECURITY**
  - 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
  - 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**
  - Enhance efforts to protect our space assets and support infrastructure from evolving cyber threats
  - Work with industry and international partners to strengthen the cyber resilience of existing and future space systems

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

3. Combat Cybercrime and Improve Incident Reporting by**:**

- **IMPROVE INCIDENT REPORTING AND RESPONSE**
  - Encourage reporting of intrusions and theft of data by all victims, especially critical infrastructure partners
- **MODERNIZE ELECTRONIC SURVEILLANCE AND COMPUTER CRIME LAWS**
  - 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**
  - Advocate for law enforcement to have effective legal tools to investigate and prosecute transnational criminal groups and modernized organized crime statutes for use against computer hacking

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

3. Combat Cybercrime and Improve Incident Reporting by**:**

- **IMPROVE APPREHENSION OF CRIMINALS LOCATED ABROAD**
  - Identify gaps and potential mechanisms for bringing foreign based cyber criminals to justice
  - Increase diplomatic and other efforts with countries to promote cooperation with legitimate extradition requests
  - 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**
  - Continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation
  - Improve international cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence
  - Lead in developing interoperable and mutually beneficial systems to encourage efficient cross-border information exchange for law enforcement purposes and reduce barriers to coordination
  - Urge effective use of existing international tools like the UN Convention Against Transnational Organized Crime

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

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

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **INCENTIVIZE AN ADAPTABLE AND SECURE TECHNOLOGY MARKETPLACE**
  - 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
  - Improve awareness and transparency of cybersecurity practices to build market demand for more secure products and services
  - Collaborate with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **PRIORITIZE INNOVATION**
  - 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
  - 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**
  - Facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure in the US
  - 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
  - Examine the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application
  - Collaborate with the private sector and civil society to understand trends in technology advancement

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **PROMOTE THE FREE FLOW OF DATA ACROSS BORDERS**
  - Continue to lead by example and push back against unjustifiable barriers to the free flow of data and digital trade
  - 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
- **MAINTAIN UNITED STATES LEADERSHIP IN EMERGING TECHNOLOGIES**
  - 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
  - Promote US 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **PROMOTE FULL-LIFECYCLE CYBERSECURITY**
  - 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
  - Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace
  - Promote foundational engineering practices to reduce systemic fragility and develop designs that degrade and recover effectively when successfully attacked
  - Promote regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries
  - Push the promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack
  - Evaluate how to improve the end-to-end lifecycle for digital identity management, including over-reliance on Social Security numbers

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

2. Foster and Protect United States Ingenuity by**:**

- **UPDATE MECHANISMS TO REVIEW FOREIGN INVESTMENT AND OPERATION IN THE UNITED STATES**
  - Formalizing and streamlining the review of Federal Communications Commission referrals for telecommunications licenses
  - Facilitate a transparent process to increase the efficiency of this review
- **MAINTAIN A STRONG AND BALANCED INTELLECTUAL PROPERTY PROTECTION SYSTEM**
  - Continue to help foster a global intellectual property rights system that provides incentives for innovation through the protection and enforcement of intellectual property rights
  - Promote protection of sensitive emerging technologies and trade secrets
  - Prevent adversarial nation states from gaining unfair advantage at the expense of American research and development
- **PROTECT THE CONFIDENTIALITY AND INTEGRITY OF AMERICAN IDEAS**
  - Work against the illicit appropriation of public and private sector technology and technical knowledge by foreign competitors, while maintaining an investor-friendly climate

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

3. Develop a Superior Cybersecurity Workforce by**:**

- **BUILD AND SUSTAIN THE TALENT PIPELINE**
  - Continue to invest in and enhance programs that build the domestic talent pipeline, from primary through postsecondary education
  - Leverage the President's proposed merit-based immigration reforms to ensure that the United States has the most competitive technology sector
- **EXPAND RE-SKILLING AND EDUCATIONAL OPPORTUNITIES FOR AMERICA'S WORKERS**
  - Work with the Congress to promote and reinvigorate educational and training opportunities to develop a robust cybersecurity workforce
- **ENHANCE THE FEDERAL CYBERSECURITY WORKFORCE**
  - 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
  - Explore appropriate options to establish distributed cybersecurity personnel under the management of DHS
  - Promote appropriate financial compensation for the US Government workforce, as well as unique training and operational opportunities

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

3. Develop a Superior Cybersecurity Workforce by**:**

- **USE EXECUTIVE AUTHORITY TO HIGHLIGHT AND REWARD TALENT**
  - Promote and magnify excellence by highlighting cybersecurity educators and cybersecurity professionals
  - Leverage public-private collaboration to develop and circulate the NICE Framework, which provides a standardized approach for identifying cybersecurity workforce gap
  - Implement actions to prepare, grow, and sustain a workforce that can defend and bolster America's critical infrastructure and innovation base

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar III – Preserve Peace Through Strength

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

Steps

1. Enhance Cyber Stability through Norms of Responsible State Behavior by**:**

- **ENCOURAGE UNIVERSAL ADHERENCE TO CYBER NORMS**
  - Encourage other nations to publicly affirm International law and voluntary non-binding norms of responsible state behavior in cyberspace) through enhanced outreach and engagement in multilateral fora

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar III – Preserve Peace Through Strength

Steps

2. Attribute and Deter Unacceptable Behavior in Cyberspace by**:**

- **LEAD WITH OBJECTIVE, COLLABORATIVE INTELLIGENCE**
  - 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
- **IMPOSE CONSEQUENCES**
  - Develop swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior
  - 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
  - work with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against our nation and interests

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar III – Preserve Peace Through Strength

Steps

2. Attribute and Deter Unacceptable Behavior in Cyberspace by**:**

- **BUILD A CYBER DETERRENCE INITIATIVE**
  - Launch an international Cyber Deterrence Initiative to build broader coalition of like-minded states and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior
  - 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**
  - 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar IV – Advance American Influence

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

Steps

1. Promote an Open, Interoperable, Reliable, and Secure Internet by**:**

- **PROTECT AND PROMOTE INTERNET FREEDOM**
  - Encourage other countries to advance Internet freedom through venues such as the Freedom Online Coalition, of which the United States is a founding member

    Note: 'Internet Freedom' in this context is defined as 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

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar IV – Advance American Influence

Steps

1. Promote an Open, Interoperable, Reliable, and Secure Internet by**:**

- **WORK WITH LIKE-MINDED COUNTRIES, INDUSTRY, ACADEMIA, AND CIVIL SOCIETY**
  - 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
  - Continue to support civil society through integrated support for technology development, digital safety training, policy advocacy, and research
- **PROMOTE A MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE**
  - Continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance (characterized by transparent, bottom-up, consensus-driven processes) prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet
  - Will defend the open, interoperable nature of the Internet in multilateral and international fora through active engagement in key organizations, such as the Internet Governance Forum, the United Nations, and the International Telecommunication Union

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar IV – Advance American Influence

Steps

1. Promote an Open, Interoperable, Reliable, and Secure Internet by**:**

- **PROMOTE INTEROPERABLE AND RELIABLE COMMUNICATIONS INFRASTRUCTURE AND INTERNET CONNECTIVITY**
  - Promote communications infrastructure and Internet connectivity that is open, interoperable, reliable, and secure
  - Support and promote open, industry-led standards activities based on sound technological principles
- **PROMOTE AND MAINTAIN MARKETS FOR UNITED STATES INGENUITY WORLDWIDE**
  - Continue to promote markets for American ingenuity overseas, including for emerging technologies that can lower the cost of security
  - Advise on infrastructure deployments, innovation, risk management, policy, and standards to further the global Internet's reach and to ensure interoperability, security, and stability
  - Work with international partners, government, industry, civil society, technologists, and academics to improve the adoption and awareness of cybersecurity best practices worldwide

Copyright © 2023 The Printer Working Group. All rights reserved.

National Cybersecurity Strategy
Pillar IV – Advance American Influence

Steps

2. Build International Cyber Capacity by**:**

- **ENHANCE CYBER CAPACITY BUILDING EFFORTS**
  - Work to strengthen the capacity and interoperability of our allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats
  - Continue to address the building blocks for organizing national efforts on cybersecurity
  - Aggressively expand efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges
  - 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

Copyright © 2023 The Printer Working Group. All rights reserved.