NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN

JULY 2023

THE WHITE HOUSE
WASHINGTON

Table of Contents

Introduction

President Biden's March 2023 National Cybersecurity Strategy lays out a bold, affirmative vision for cyberspace. It outlines a path for achieving two significant shifts: the need for more capable actors in cyberspace to bear more of the responsibility for cybersecurity and the need to increase incentives to make investments in long term-resilience.

Achieving the President's cybersecurity vision requires coordinated action across the United States Government and American society. The National Cybersecurity Strategy Implementation Plan is a roadmap for this effort. While it does not intend to capture all cybersecurity activities being carried out by agencies, it describes more than 65 high-impact initiatives requiring executive visibility and interagency coordination that the Federal government will carry out to achieve the Strategy's objectives. Each initiative is assigned to a responsible agency and is associated with a timeline for completion. Some of these initiatives are already underway and will be completed by the end of Fiscal Year 2023. The Office of the National Cyber Director will work with the Office of Management and Budget to ensure funding proposals in the President's Budget Request are aligned with activities in the Implementation Plan.

This is the first iteration of the Implementation Plan, which is a living document that will be updated annually. Initiatives will be added as the evolving cyber landscape demands and removed after completion. The Office of the National Cyber Director will coordinate this work and report to the President and to Congress on the status of implementation.

The United States Government will only succeed in implementing the National Cybersecurity Strategy through close collaboration with the private sector; civil society; state, local, Tribal, and territorial governments; international partners; and Congress. Agencies will work with interested stakeholders to implement the initiatives of this Plan and build new partnerships where possible. The Administration will continue to refine Implementation Plan initiatives based on stakeholder feedback and assessments of their effectiveness.

Implementation Plan Reading Guide

The Implementation Plan is structured by pillar and strategic objective, to align with the National Cybersecurity Strategy, which has five pillars and 27 strategic objectives. The fields presented for each initiative are:

Pillar – The Pillar under which the initiative falls.

Strategic Objective – The Strategic Objective associated with the initiative.

Initiative Number – A unique number associated with the specific initiative in the form of <Pillar>.<Strategic Objective>.<Initiative Number>.

Initiative Title – The title of an action that will support the overall outcome of the Strategic Objective.

Initiative Description – An explanation of the activities associated with the action.

National Cybersecurity Strategy (NCS) Reference – The specific language from the Strategy tied to the initiative.

Responsible Agency – The Federal agency responsible for leading the initiative with other stakeholders.

Contributing Entities – Where applicable, Federal departments or agencies that have a significant role in the development and execution of the initiative, including by contributing expertise or resources, engaging in complementary efforts, or coordinating on elements of a program. This is not intended to be a comprehensive list of all agencies with equities in an initiative.

Completion Date – Estimated completion date by quarter within the United States Government fiscal year.

Roll-Up of Implementation Plan Initiatives

Pillar One: Defend Critical Infrastructure

1.1 Establish Cybersecurity Requirements to Support National Security and Public Safety

- 1.1.1 Establish an initiative on cyber regulatory harmonization
- 1.1.2 Set cybersecurity requirements across critical infrastructure sectors
- 1.1.3 Increase agency use of frameworks and international standards to inform regulatory alignment

1.2 Scale Public-Private Collaboration

- 1.2.1 Scale public-private partnerships to drive development and adoption of secure-by-design and secure-by-default technology
- 1.2.2 Provide recommendations for the designation of critical infrastructure sectors and SRMAs
- 1.2.3 Evaluate how CISA can leverage existing reporting mechanisms or the potential creation of a single portal to integrate and operationalize SRMAs' sector-specific systems and processes
- 1.2.4 Investigate opportunities for new and improved information sharing and collaboration platforms, processes, and mechanisms
- 1.2.5 Establish an SRMA support capability

1.3 Integrate Federal Cybersecurity Centers

- 1.3.1 Assess and improve Federal Cybersecurity Centers' and related cyber centers' capabilities and plans necessary for collaboration at speed and scale

1.4 Update Federal Incident Response Plans and Processes

- 1.4.1 Update the National Cyber Incident Response Plan (NCIRP)
- 1.4.2 Issue final Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule
- 1.4.3 Develop exercise scenarios to improve cyber incident response
- 1.4.4 Draft legislation to codify the Cyber Safety Review Board (CSRB) with the required authorities

1.5 Modernize Federal Defenses

- 1.5.1 Secure unclassified Federal Civilian Executive Branch (FCEB) systems
- 1.5.2 Modernize Federal Civilian Executive Branch (FCEB) technology
- 1.5.3 Secure National Security Systems (NSS) at Federal Civilian Executive Branch (FCEB) agencies

Pillar Two: Disrupt and Dismantle Threat Actors

2.1 Integrate Federal Disruption Activities

- 2.1.1 Publish an updated DOD Cyber Strategy
- 2.1.2 Strengthen the National Cyber Investigative Joint Task Force (NCIJTF) capacity
- 2.1.3 Expand organizational platforms dedicated to disruption campaigns
- 2.1.4 Propose legislation to disrupt and deter cybercrime and cyber-enabled crime
- 2.1.5 Increase speed and scale of disruption operations

2.2 Enhance Public-Private Operational Collaboration to Disrupt Adversaries

- 2.2.1 Identify mechanisms for increased adversarial disruption through public-private operational collaboration

2.3 Increase the Speed and Scale of Intelligence Sharing and Victim Notification

- 2.3.1 Identify and operationalize sector-specific intelligence needs and priorities
- 2.3.2 Remove barriers to delivering cyber threat intelligence and data to critical infrastructure owners and operators

2.4 Prevent Abuse of U.S.-Based Infrastructure

- 2.4.1 Publish a Notice of Proposed Rulemaking on requirements, standards, and procedures for Infrastructure-as-a-Service (IaaS) providers and resellers

2.5 Counter Cybercrime, Defeat Ransomware

- 2.5.1 Disincentivize safe havens for ransomware criminals
- 2.5.2 Disrupt ransomware crimes
- 2.5.3 Investigate ransomware crimes and disrupt the ransomware ecosystem
- 2.5.4 Support private sector and state, local, Tribal, and territorial (SLTT) efforts to mitigate ransomware risk
- 2.5.5 Support other countries' efforts to adopt and implement the global anti-money laundering/countering the financing of terrorism (AML/CFT) standards for virtual asset service providers

Pillar Three: Shape Market Forces to Drive Security and Resilience

★ ★ ★ ★ ★ ★

Pillar Four: Invest in A Resilient Future

★ ★ ★ ★ ★ ★

Pillar Five: Forge International Partnerships to Pursue Shared Goals

5.1 Build Coalitions to Counter Threats to Our Digital Ecosystem
- 5.1.1 Create interagency teams for regional cyber collaboration and coordination
- 5.1.2 Publish an International Cyberspace and Digital Policy Strategy
- 5.1.3 Strengthen Federal law enforcement collaboration mechanisms with allies and partners
- 5.1.4 Regional cyber hubs study

5.2 Strengthen International Partner Capacity
- 5.2.1 Strengthen international partners' cyber capacity
- 5.2.2 Expand international partners' cyber capacity through operational law enforcement collaboration

5.3 Expand U.S. Ability to Assist Allies and Partners
- 5.3.1 Establish flexible foreign assistance mechanisms to provide cyber incident response support quickly

5.4 Build Coalitions to Reinforce Global Norms of Responsible State Behavior
- 5.4.1 Hold irresponsible states accountable when they fail to uphold their commitments

5.5 Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services
- 5.5.1 Promote the development of secure and trustworthy information and communication technology (ICT) networks and services
- 5.5.2 Promote a more diverse and resilient supply chain of trustworthy information and communication (ICT) vendors
- 5.5.3 Begin administering the Public Wireless Supply Chain Innovation Fund (PWSCIF)
- 5.5.4 Promulgate and amplify Cybersecurity Supply Chain Risk Management (C-SCRM) key practices across and within critical infrastructure sectors

Implementation-wide Initiatives

6.1 Assessing Effectiveness

- 6.1.1 Report progress and effectiveness on implementing the National Cybersecurity Strategy
- 6.1.2 Apply lessons learned to the National Cybersecurity Strategy implementation
- 6.1.3 Align budgetary guidance with National Cybersecurity Strategy implementation

Pillar One: Defend Critical Infrastructure

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

Initiative Number: 1.1.1

Initiative Title: Establish an initiative on cyber regulatory harmonization

Initiative Description

The Office of the National Cyber Director (ONCD), in coordination with OMB, will work with independent and executive branch regulators, including through the Cybersecurity Forum for Independent and Executive Branch Regulators, to identify opportunities to harmonize baseline cybersecurity requirements for critical infrastructure. Through a request for information, ONCD will also engage non-governmental stakeholders to understand existing challenges with regulatory overlap and explore a framework for reciprocity for baseline requirements.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: FCC, OMB

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 1.1.2

Initiative Title: Set cybersecurity requirements across critical infrastructure sectors

Initiative Description

Through the ongoing National Security Council-led policymaking process, SRMAs and regulators will analyze the cyber risk in their industries and outline how they will use their existing authorities to establish cyber requirements that mitigate risk in their sector, account for sector-specific needs, identify gaps in authorities, and develop proposals to close them.

NCS Reference

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…the Administration will work with Congress to close them.

Responsible Agency: NSC

Contributing Entities: SRMAs, ONCD

Completion Date: 2Q FY25

Initiative Number: 1.1.3

Initiative Title: Increase agency use of frameworks and international standards to inform regulatory alignment

Initiative Description

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is refined, improved, and evolves over time. Updates help the performance-based Framework keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice. NIST is developing a significant update to the Framework: CSF 2.0. NIST will issue the final CSF 2.0 and provide technical assistance on alignment of regulations with international standards and the NIST CSF, as requested by Federal agencies.

NCS Reference

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...

Responsible Agency: NIST

Contributing Entities: CISA, SRMAs

Completion Date: 1Q FY25

★ ★ ★ ★ ★ ★

Strategic Objective 1.2: Scale Public-Private Collaboration

Initiative Number: 1.2.1

Initiative Title: Scale public-private partnerships to drive development and adoption of secure-by-design and secure-by-default technology

Initiative Description

The Cybersecurity and Infrastructure Security Agency (CISA) will lead public-private partnerships with technology manufacturers, educators, non-profit organizations, academia, the open-source software community, and others to drive the development and adoption of software and hardware that is secure-by-design and secure-by-default. CISA, working with NIST, other Federal agencies, including SRMAs, as appropriate, and the private sector will develop secure-by-design and secure-by-default principles and practices that first leverage existing and relevant international, industry, and government standards and practices. CISA will identify barriers to adoption for such principles and best practices, and will work to drive collective action to adopt these principles across the private sector. In the case that gaps between secure-by-design and secure-by-default principles and existing standards and practices are identified, CISA, NIST, NSF, and other Federal agencies, including SRMAs, as appropriate, will lead open and transparent public-private partnerships to fill those gaps.

NCS Reference

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.

Responsible Agency: CISA

Contributing Entities: NIST, NSF, SRMAs

Completion Date: 4Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 1.2.2

Initiative Title: Provide recommendations for the designation of critical infrastructure sectors and SRMAs

Initiative Description

The Federal Senior Leadership Council shall review SRMAs capabilities through the agreed upon SRMA criteria, will consult private-sector partners as appropriate, and will provide a recommendation on critical infrastructure sectors' SRMAs to the Secretary of Homeland Security.

NCS Reference

The Federal Government will continue to enhance coordination between CISA and other SRMAs.

Responsible Agency: CISA

Contributing Entities: SRMAs, NSC, ONCD

Completion Date: 1Q FY24

Initiative Number: 1.2.3

Initiative Title: Evaluate how CISA can leverage existing reporting mechanisms or the potential creation of a single portal to integrate and operationalize SRMAs' sector-specific systems and processes

Initiative Description

The Cybersecurity and Infrastructure Security Agency will work with SRMAs to understand where gaps exist in information sharing and understand requirements for an interoperable system for information exchange among SRMAs and other Federal partners. Where SRMAs do not have robust information sharing capabilities already in place, CISA will work with them to develop a process to mature their capabilities.

NCS Reference

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.

Responsible Agency: CISA

Contributing Entities: DOJ, FBI, NSA, SRMAs

Completion Date: 3Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 1.2.4

Initiative Title: Investigate opportunities for new and improved information sharing and collaboration platforms, processes, and mechanisms

Initiative Description

The Cybersecurity and Infrastructure Security Agency will lead a cross sector effort to review public-private collaboration mechanisms. SRMAs, in coordination with CISA as appropriate, will represent the activities in their sectors such as Sector Coordinating Councils, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), emerging sector collaboration initiatives, and other entities to deliver to CISA for the development of a maturity model for public-private collaboration.

NCS Reference

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.

Responsible Agency: CISA

Contributing Entities: SRMAs

Completion Date: 1Q FY26

Initiative Number: 1.2.5

Initiative Title: Establish an SRMA support capability

Initiative Description

The Cybersecurity and Infrastructure Security Agency will establish and codify an SRMA Support Office Capability to serve as the single point of contact for supporting all SRMAs. The office will coordinate the provision of CISA services for each SRMA, depending on its capabilities. CISA will work with each SRMA to define its needs and priorities for support from the office, to include evaluating options and opportunities for shared services, and use this information to update CISA's services catalog, as necessary.

NCS Reference

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.

Responsible Agency: CISA

Contributing Entities: SRMAs, NSC

Completion Date: 2Q FY25

Strategic Objective 1.3: Integrate Federal Cybersecurity Centers

Initiative Number: 1.3.1

Initiative Title: Assess and improve Federal Cybersecurity Centers' and related cyber centers' capabilities and plans necessary for collaboration at speed and scale

Initiative Description

The Office of the National Cyber Director will conduct a review of Federal Cybersecurity Centers and related cyber centers to identify gaps in capabilities and other key findings.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: OMB

Completion Date: 4Q FY23

Strategic Objective 1.4: Update Federal Incident Response Plans and Processes

Initiative Number: 1.4.1

Initiative Title: Update the National Cyber Incident Response Plan (NCIRP)

Initiative Description

The Cybersecurity and Infrastructure Security Agency, in coordination with ONCD, will lead a process to update the National Cyber Incident Response Plan (NCIRP) – which is subordinate to Presidential Policy Directive 41 – to strengthen processes, procedures, and systems to more fully realize the policy that "a call to one is a call to all." The NCIRP update will also include clear guidance to external partners on the roles and capabilities of Federal agencies in incident response and recovery.

NCS Reference

CISA will lead a process to update the National Cyber Incident Response Plan (NCIRP)…

Responsible Agency: CISA

Contributing Entities: DOJ, FBI, SRMAs, USSS, ONCD

Completion Date: 1Q FY25

★ ★ ★ ★ ★ ★

Initiative Number: 1.4.2

Initiative Title: Issue final Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule

Initiative Description

The Cybersecurity and Infrastructure Security Agency will consult with SRMAs, DOJ, and other Federal agencies to implement CIRCIA. CISA will publish the CIRCIA Notice of Proposed Rulemaking and Final Rule per the statutory requirements, and develop the processes to advance effective actioning of incident reports to include sharing of incident reports with appropriate agencies.

NCS Reference

CISA will consult with SRMAs, the Department of Justice (DOJ), and other Federal agencies during the CIRCIA rule-making and implementation…

Responsible Agency: CISA

Contributing Entities: DOJ, FBI, SRMAs, USSS

Completion Date: 4Q FY25

Initiative Number: 1.4.3

Initiative Title: Develop exercise scenarios to improve cyber incident response

Initiative Description

The Office of the National Cyber Director will work with the interagency and other relevant stakeholders to develop multiple tabletop exercise scenarios to allow the interagency to continue to refine delivering a whole-of-government response to a cyber incident.

NCS Reference

When Federal assistance is required, the Federal Government must present a unified, coordinated, whole-of-government response.

Responsible Agency: ONCD

Contributing Entities: DHS

Completion Date: 1Q FY24

Initiative Number: 1.4.4

Initiative Title: Draft legislation to codify the Cyber Safety Review Board (CSRB) with the required authorities

Initiative Description

The Department of Homeland Security will work with Congress to codify the CSRB.

NCS Reference

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.

Responsible Agency: DHS

Contributing Entities: DOD, DOJ, CISA, FBI, NSA, OMB, ONCD

Completion Date: 2Q FY23

Strategic Objective 1.5: Modernize Federal Defenses

Initiative Number: 1.5.1

Initiative Title: Secure unclassified Federal Civilian Executive Branch (FCEB) systems

Initiative Description

The Office of Management and Budget, in coordination with CISA, will develop a plan of action to secure unclassified FCEB systems through collective operational defense and to foster expanded use of centralized shared services, enterprise license agreements, and software supply chain risk mitigation.

NCS Reference

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.

Responsible Agency: OMB

Contributing Entities: CISA, NIST, ONCD

Completion Date: 2Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 1.5.2

Initiative Title: Modernize Federal Civilian Executive Branch (FCEB) technology

Initiative Description

The Office of Management and Budget 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.

NCS Reference

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.

Responsible Agency: OMB

Contributing Entities: CISA, GSA, ONCD

Completion Date: 4Q FY24

Initiative Number: 1.5.3

Initiative Title: Secure National Security Systems (NSS) at Federal Civilian Executive Branch (FCEB) agencies

Initiative Description

The National Security Agency, in fulfilling the responsibilities of the National Manager for National Security Systems (NSS), will develop and execute a plan to address the security of NSS at FCEB agencies.

NCS Reference

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 National Security Memorandum (NSM)-8.

Responsible Agency: NSA

Contributing Entities: OMB, ONCD

Completion Date: 4Q FY24

Pillar Two: Disrupt and Dismantle Threat Actors

Strategic Objective 2.1: Integrate Federal Disruption Activities

Initiative Number: 2.1.1

Initiative Title: Publish an updated DOD Cyber Strategy

Initiative Description

The Department of Defense will develop an updated Cyber Strategy aligned with the National Security Strategy, National Defense Strategy, and National Cybersecurity Strategy to focus on challenges posed by nation-states and other malicious actors whose capabilities or campaigns pose a strategic-level threat to the United States and its interests.

NCS Reference

…DOD will develop an updated departmental cyber strategy aligned with the National Security Strategy, National Defense Strategy, and this National Cybersecurity Strategy.

Responsible Agency: DOD

Completion Date: 1Q FY24

Initiative Number: 2.1.2

Initiative Title: Strengthen the National Cyber Investigative Joint Task Force (NCIJTF) capacity

Initiative Description

The NCIJTF will strengthen its capacity to coordinate takedown and disruption campaigns with greater speed, scale, and frequency.

NCS Reference

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.

Responsible Agency: FBI

Contributing Entities: DOJ

Completion Date: 4Q FY25

Initiative Number: 2.1.3

Initiative Title: Expand organizational platforms dedicated to disruption campaigns

Initiative Description

The Department of Justice will increase the volume and speed of disruption campaigns against cybercriminals, nation-state adversaries, and associated enablers (e.g., money launderers) by expanding its organizational platforms dedicated to such threats and increasing the number of qualified attorneys dedicated to cyber work.

NCS Reference

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.

Responsible Agency: DOJ

Completion Date: 1Q FY25

Initiative Number: 2.1.4

Initiative Title: Propose legislation to disrupt and deter cybercrime and cyber-enabled crime

Initiative Description

The Department of Justice will work with interagency partners to develop a targeted set of legislative proposals that, if enacted, will enhance the U.S. Government's capacity to disrupt and deter cybercrime.

NCS Reference

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.

Responsible Agency: DOJ

Contributing Entities: DHS, Treasury, CISA, FBI, USSS, ONCD

Completion Date: 4Q FY23

★ ★ ★ ★ ★ ★

Initiative Number: 2.1.5

Initiative Title: Increase speed and scale of disruption operations

Initiative Description

The National Cyber Investigative Joint Task Force, law enforcement agencies, U.S. Cyber Command, NSA, and other elements of the intelligence community will lead the development of a menu of options for coordinating and executing disruption operations to increase the speed and scale of these operations.

NCS Reference

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.

Responsible Agency: FBI

Completion Date: 2Q FY24

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

Initiative Number: 2.2.1

Initiative Title: Identify mechanisms for increased adversarial disruption through public-private operational collaboration

Initiative Description

The Office of the National Cyber Director, in collaboration with the interagency and private sector partners, will identify opportunities to leverage existing mechanisms to improve operational collaboration with the goal of increasing disruption of malicious cyber actors.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: DOJ, CISA, FBI, NSA, USSS

Completion Date: 2Q FY24

★ ★ ★ ★ ★ ★

Strategic Objective 2.3: Increase the Speed and Scale of Intelligence Sharing and Victim Notification

Initiative Number: 2.3.1

Initiative Title: Identify and operationalize sector-specific intelligence needs and priorities

Initiative Description

Consistent with the requirement set forth in the Fiscal Year 2021 National Defense Authorization Act Section 9002(c)(1), the National Security Council will lead a policymaking process to establish an agreed-upon approach for SRMAs to identify sector-specific intelligence needs and priorities.

NCS Reference

SRMAs, in coordination with CISA, law enforcement agencies, and the Cyber Threat Intelligence Integration Center (CTIIC), will identify intelligence needs and priorities within their sector and develop processes to share warnings, technical indicators…

Responsible Agency: NSC

Contributing Entities: DHS, DOJ, ODNI, CIA, CISA, FBI, NSA, SRMAs, USSS

Completion Date: 1Q FY25

Initiative Number: 2.3.2

Initiative Title: Remove barriers to delivering cyber threat intelligence and data to critical infrastructure owners and operators

Initiative Description

Leveraging the deliverables and lessons learned from EO 13636, Sec. 4 implementation, the Office of the Director of National Intelligence will, in coordination with DOJ and DHS, review policies and procedures for sharing cyber threat intelligence with critical infrastructure owners and operators and evaluate the need for expanding clearances and intelligence access to enable this.

NCS Reference

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.

Responsible Agency: ODNI

Contributing Entities: DOD, DHS, DOJ, FBI, NSA, NSC, ONCD

Completion Date: 3Q FY24

★ ★ ★ ★ ★ ★

Strategic Objective 2.4: Prevent Abuse of U.S.-Based Infrastructure

Initiative Number: 2.4.1

Initiative Title: Publish a Notice of Proposed Rulemaking on requirements, standards, and procedures for Infrastructure-as-a-Service (IaaS) providers and resellers

Initiative Description

The Department of Commerce will publish a Notice of Proposed Rulemaking implementing EO 13984 that lays out requirements for IaaS providers and resellers as well as standards and procedures for determining what risk-based prevention approach is sufficient to qualify for an exemption.

NCS Reference

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."

Responsible Agency: Commerce

Contributing Entities: DHS, DOJ, ODNI, FBI

Completion Date: 4Q FY23

★ ★ ★ ★ ★ ★

Strategic Objective 2.5: Counter Cybercrime, Defeat Ransomware

Initiative Number: 2.5.1

Initiative Title: Disincentivize safe havens for ransomware criminals

Initiative Description

The Department of State, in coordination with the Joint Ransomware Task Force (JRTF) (co-chaired by FBI and CISA), will work with DOJ and other stakeholders to develop an international engagement plan to discourage nations from acting as safe havens for ransomware criminals and strengthen international cooperation in countering transnational cybercrime.

NCS Reference

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…isolate those countries that provide safe havens for criminals…

Responsible Agency: State

Contributing Entities: DHS, DOJ, CISA, FBI

Completion Date: 4Q FY23

Initiative Number: 2.5.2

Initiative Title: Disrupt ransomware crimes

Initiative Description

The FBI, in coordination with the Joint Ransomware Task Force (JRTF) (co-chaired by FBI and CISA), will work with U.S. Secret Service, DOJ, CISA and other Federal, international, and private sector partners to carry out disruption operations against the ransomware ecosystem, including virtual asset providers that enable laundering of ransomware proceeds and web fora offering initial access credentials or other material support for ransomware activities.

NCS Reference

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...; (2) investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors; ... and (4) addressing the abuse of virtual currency to launder ransomware proceeds.

The Joint Ransomware Task Force (JRTF) will coordinate, deconflict, and synchronize existing interagency efforts to disrupt ransomware operations....

Responsible Agency: FBI

Contributing Entities: DOJ, CISA, NSA, USSS

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 2.5.3

Initiative Title: Investigate ransomware crimes and disrupt the ransomware ecosystem

Initiative Description

The Department of Justice, leveraging mutual legal assistance channels and domestic legal process, forfeiture proceedings, and criminal charging authorities, will strengthen its capacity to work with Federal, international and private sector partners to plan, coordinate, and execute disruption operations against the ransomware ecosystem, including virtual asset providers that enable money-laundering proceeds and web fora offering initial access credentials or other material support for ransomware activities.

NCS Reference

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 . . .; (2) investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors; and… (4) addressing the abuse of virtual currency to launder ransomware proceeds.

Responsible Agency: DOJ

Completion Date: 2Q FY24

Initiative Number: 2.5.4

Initiative Title: Support private sector and state, local, Tribal, and territorial (SLTT) efforts to mitigate ransomware risk

Initiative Description

The Cybersecurity and Infrastructure Security Agency, in coordination with the JRTF (co-chaired by CISA and FBI), SRMAs, and other stakeholders, will offer resources such as training, cybersecurity services, technical assessments, pre-attack planning, and incident response to critical infrastructure organizations, SLTT, and other high-risk targets of ransomware to reduce the likelihood of impact and the scale and duration of impacts when they occur.

NCS Reference

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... (3) bolstering critical infrastructure resilience to withstand ransomware attacks…

The Joint Ransomware Task Force (JRTF) will.... provide support to private sector and SLTT efforts to increase their protections against ransomware.

Responsible Agency: CISA

Contributing Entities: FBI, SRMAs, USSS, NSC

Completion Date: 1Q FY25

★ ★ ★ ★ ★ ★

Initiative Number: 2.5.5

Initiative Title: Support other countries' efforts to adopt and implement the global anti-money laundering/countering the financing of terrorism (AML/CFT) standards for virtual asset service providers

Initiative Description

The Department of the Treasury will lead government stakeholders, including DOJ, State, and other interagency participants, and will work with international partners bilaterally and through the Treasury-led delegation to the Financial Action Task Force (FATF) to accelerate global adoption and implementation of anti-money laundering and countering the financing of terrorism (AML/CFT) standards and supervision for virtual asset service providers, including disrupting providers that enable laundering of ransomware payments. The U.S. will continue to draft and contribute to Recommendation 15-related publications, including planned materials for publication in early and mid-2024. This includes providing technical assistance to low-capacity countries and encouraging other FATF members to provide similar support.

NCS Reference

…the United States will support implementation of international AML/CFT standards to mitigate the use of cryptocurrencies for illicit activities…

Responsible Agency: Treasury

Contributing Entities: DOJ, State, USSS, NSC

Completion Date: 4Q FY24

Pillar Three: Shape Market Forces to Drive Security and Resilience

Strategic Objective 3.2: Drive the Development of Secure IoT Devices

Initiative Number: 3.2.1

Initiative Title: Implement Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020

Initiative Description

The Office of Management and Budget, through the Office of Federal Procurement Policy, will work with the Federal Acquisition Regulatory Council to propose FAR changes in line with the Internet of Things Cybersecurity Improvement Act of 2020.

NCS Reference

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.

Responsible Agency: OMB

Completion Date: 4Q FY23

Initiative Number: 3.2.2

Initiative Title: Initiate a U.S. Government IoT security labeling program

Initiative Description

Following the October 2022 White House event on this topic, the National Security Council will identify the broad contours of a U.S. Government Internet of Things (IoT) security labeling program and an agency to lead it.

NCS Reference

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."

Responsible Agency: NSC

Completion Date: 4Q FY23

★ ★ ★ ★ ★ ★

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

Initiative Number: 3.3.1

Initiative Title: Explore approaches to develop a long-term, flexible, and enduring software liability framework

Initiative Description

The Office of the National Cyber Director, working with stakeholders in academia and civil society, will host a legal symposium to explore different approaches to a software liability framework that draw from different areas of regulatory law and reflect inputs from computer scientists as to the extent that software liability may or may not be like these other regimes.

NCS Reference

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... The Administration will work with Congress and the private sector to develop legislation establishing a liability regime for software products and services.

Responsible Agency: ONCD

Completion Date: 2Q FY24

Initiative Number: 3.3.2

Initiative Title: Advance software bill of materials (SBOM) and mitigate the risk of unsupported software

Initiative Description

In order to collect data on the usage of unsupported software in critical infrastructure, the Cybersecurity and Infrastructure Security Agency will work with key stakeholders, including SRMAs, to identify and reduce gaps in SBOM scale and implementation. CISA will also explore requirements for a globally-accessible database for end-of-life/end-of-support software and convene an international staff-level working group on SBOM.

NCS Reference

The Administration will .... 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.

Responsible Agency: CISA

Completion Date: 2Q FY25

Initiative Number: 3.3.3

Initiative Title: Coordinated vulnerability disclosure

Initiative Description

The Cybersecurity and Infrastructure Security Agency will work to build domestic and international support for an expectation of coordinated vulnerability disclosure among public and private entities, across all technology types and sectors, including through the creation of an international vulnerability coordinator community of practice. This will include supporting international institutions, including international Computer Emergency Response Teams and other community-driven organizations, to build global awareness and capacity around coordinated vulnerability disclosure.

NCS Reference

To further incentivize the adoption of secure software development practices, the Administration will encourage coordinated vulnerability disclosure across all technology types and sectors…

Responsible Agency: CISA

Contributing Entities: State

Completion Date: 4Q FY25

Strategic Objective 3.4: Use Federal Grants and Other Incentives to Build in Security

Initiative Number: 3.4.1

Initiative Title: Leverage Federal grants to improve infrastructure cybersecurity

Initiative Description

The Office of the National Cyber Director will develop materials to clarify, facilitate, and encourage incorporation of cybersecurity equities into Federal grant projects.

NCS Reference

Through programs funded by the Bipartisan Infrastructure Law…, 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.

Responsible Agency: ONCD

Contributing Entities: CISA, OMB

Completion Date: 4Q FY23

★ ★ ★ ★ ★ ★

Initiative Number: 3.4.2

Initiative Title: Prioritize funding for cybersecurity research

Initiative Description

The Office of Science and Technology Policy, in coordination with ONCD and OMB, will, through the Fiscal Year 2025 budget process, encourage prioritization of cybersecurity research, development, and demonstrations aimed at strengthening security and resilience for critical infrastructure.

NCS Reference

The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience.

Responsible Agency: OSTP

Contributing Entities: OMB, ONCD

Completion Date: 4Q FY23

Initiative Number: 3.4.3

Initiative Title: Prioritize cybersecurity research, development, and demonstration on social, behavioral, and economic research in cybersecurity

Initiative Description

Through grant awards in Fiscal Year 2024, the National Science Foundation will invest in increasing understanding of individual and societal impacts on cybersecurity, and the impacts of cybersecurity on individuals and society, through research in cyber economics, human factors, information integrity, and related topics.

NCS Reference

The Federal Government will also prioritize funding for cybersecurity research, development, and demonstration (RD&D) programs aimed at strengthening critical infrastructure cybersecurity and resilience.

Responsible Agency: NSF

Completion Date: 4Q FY24

★ ★ ★ ★ ★ ★

Strategic Objective 3.5: Leverage Federal Procurement to Improve Accountability

Initiative Number: 3.5.1

Initiative Title: Implement Federal Acquisition Regulation (FAR) changes required under EO 14028

Initiative Description

The Office of Management and Budget, acting through the Office of Federal Procurement Policy, will work with the Federal Acquisition Regulatory Council to propose changes to the FAR required under EO 14028. Through the release of draft rules (cybersecurity incident reporting, standardizing cybersecurity contract requirements, and secure software) public comment will be considered before the changes are finalized.

NCS Reference

EO 14028, "Improving the Nation's Cybersecurity," expands upon this approach, ensuring that contract requirements for cybersecurity are strengthened and standardized across Federal agencies.

Responsible Agency: OMB

Completion Date: 1Q FY24

Initiative Number: 3.5.2

Initiative Title: Leverage the False Claims Act to improve vendor cybersecurity

Initiative Description

The Department of Justice will expand efforts to identify, pursue, and deter knowing failures to comply with cybersecurity requirements in Federal contracts and grants with the aim of building resilience, increasing vulnerability disclosures, reducing the competitive disadvantage for responsible vendors, and recovering damages for affected Federal programs and agencies.

NCS Reference

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.

Responsible Agency: DOJ

Completion Date: 4Q FY25

★ ★ ★ ★ ★ ★

Strategic Objective 3.6: Explore a Federal Cyber Insurance Backstop

Initiative Number: 3.6.1

Initiative Title: Assess the need for a Federal insurance response to a catastrophic cyber event

Initiative Description

The Department of the Treasury's Federal Insurance Office, in coordination with CISA and ONCD, will assess the need for a Federal insurance response to catastrophic cyber events that would support the existing cyber insurance market.

NCS Reference

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.

Responsible Agency: Treasury

Contributing Entities: CISA, ONCD

Completion Date: 1Q FY24

Pillar Four: Invest in a Resilient Future

Strategic Objective 4.1: Secure the Technical Foundation of the Internet

Initiative Number: 4.1.1

Initiative Title: Lead the adoption of network security best practices

Initiative Description

The Office of Management and Budget, in coordination with CISA will work with Federal agencies to prioritize encryption of Domain Name System requests, as aligned with the zero trust strategy and maturity model (M-22-09).

NCS Reference

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... 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.

Responsible Agency: OMB

Contributing Entities: CISA, ONCD

Completion Date: 2Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 4.1.2

Initiative Title: Promote open-source software security and the adoption of memory safe programming languages

Initiative Description

The Office of the National Cyber Director will establish an Open-Source Software Security Initiative (OS3I) to champion the adoption of memory safe programming languages and open-source software security. As part of this initiative, CISA will work with OS3I and the open-source software community to enable the secure usage of open-source software in the Federal Government and critical infrastructure, and to raise the security baseline of the open-source software ecosystem. CISA will also develop close partnerships with open-source software community members and integrate into various community efforts.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: CISA, NSF, OMB

Completion Date: 1Q FY24

Initiative Number: 4.1.3

Initiative Title: Accelerate development, standardization, and adoption of foundational Internet infrastructure capabilities and technologies

Initiative Description

Consistent with the National Standards Strategy, the National Institute of Standards and Technology will convene the Interagency International Cybersecurity Standardization Working Group to coordinate on major issues in international cybersecurity standardization and enhance U.S. Federal agency participation in the process.

NCS Reference

By supporting non-governmental Standards Developing Organizations, 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.

Responsible Agency: NIST

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 4.1.4

Initiative Title: Accelerate the development and standardization, and support the adoption, of foundational Internet infrastructure capabilities and technologies

Initiative Description

The National Institute of Standards and Technology will collaborate with the interagency, industry, academia, and other communities to address Border Gateway Protocol (BGP) and Internet Protocol Version 6 (IPv6) security gaps by driving development, commercialization, and adoption of international standards.

NCS Reference

The Internet is critical to our future but retains the fundamental structure of its past. ...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… 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.

Responsible Agency: NIST

Completion Date: 4Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 4.1.5

Initiative Title: Collaborate with key stakeholders to drive secure Internet routing

Initiative Description

The Office of the National Cyber Director, in conjunction with key stakeholders and appropriate Federal Government entities, will develop a roadmap to increase the adoption of secure Internet routing techniques and technology by: (1) identifying security challenges; (2) exploring approaches and options to address internet routing and BGP security concerns; (3) identifying and informing the development of best practices; (4) identifying needed research and development; and (5) identifying barriers to adoption and alternate mitigation approaches.

NCS Reference

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…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.

Responsible Agency: ONCD

Contributing Entities: DOJ, CISA, FCC, NIST, NSA, NTIA, OSTP

Completion Date: 3Q FY24

★ ★ ★ ★ ★ ★

Strategic Objective 4.2: Reinvigorate Federal Research and Development for Cybersecurity

Initiative Number: 4.2.1

Initiative Title: Accelerate maturity, adoption, and security of memory safe programming languages

Initiative Description

Through the Federal Cybersecurity R&D Strategic Plan, the Office of Science and Technology Policy will work with NSF, NIST, grant-making agencies, OS3I, and other relevant Federal partners to prioritize investments to accelerate the maturity, adoption, and security of memory safe programming languages in applications, operating systems, and critical infrastructure.

NCS Reference

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... 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.

Responsible Agency: OSTP

Contributing Entities: DHS, CISA, NIST, NSF

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Strategic Objective 4.3: Prepare for Our Post-Quantum Future

Initiative Number: 4.3.1

Initiative Title: Implement National Security Memorandum-10

Initiative Description

The Office of Management and Budget and the National Manager for National Security Systems, in coordination with ONCD, will continue to prioritize implementation of National Security Memorandum-10 and transitioning vulnerable public networks and systems to quantum-resistant cryptography-based environments, focusing first on Federal information systems and NSS. OMB will work with NIST to develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

NCS Reference

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.

Responsible Agency: OMB

Contributing Entities: NSA, ONCD

Completion Date: 1Q FY25

★ ★ ★ ★ ★ ★

Initiative Number: 4.3.2

Initiative Title: Implement NSM-10 for National Security Systems (NSS)

Initiative Description

Implement the transition of NSS to quantum-resistant cryptography.

NCS Reference

The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography (QRC)-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Responsible Agency: NSA

Contributing Entities: DOD, ODNI

Completion Date: 3Q FY25

Initiative Number: 4.3.3

Initiative Title: Standardize, and support transition to, post-quantum cryptographic algorithms

Initiative Description

The National Institute of Standards and Technology will finalize its process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. New public-key cryptography standards will specify one or more additional unclassified, publicly-disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

NCS Reference

To balance the promotion and advancement of quantum computing against threats posted to digital systems, National Security Memorandum (NSM) 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes responsibilities and oversight to enable a timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography.

Responsible Agency: NIST

Completion Date: 1Q FY25

★ ★ ★ ★ ★ ★

Strategic Objective 4.4: Secure Our Clean Energy Future

Initiative Number: 4.4.1

Initiative Title: Drive adoption of cyber secure-by-design principles by incorporating them into Federal projects

Initiative Description

The Department of Energy, working with ONCD and CISA, will work with stakeholders to identify and implement cyber secure-by-design pilot projects, identify economic incentives for cyber secure-by-design, identify needed technology vehicles to apply cyber secure-by-design principles, and measure progress on national implementation of cyber secure-by-design efforts for critical infrastructure.

NCS Reference

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.

Responsible Agency: DOE

Contributing Entities: CISA, NIST, ONCD

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 4.4.2

Initiative Title: Develop a plan to ensure the digital ecosystem can support and deliver the U.S. government's decarbonization goals

Initiative Description

Leveraging the Department of Energy's leadership and in close collaboration with the Executive Office of the President, the Office of the National Cyber Director will develop a plan to ensure that the digital ecosystem is prepared to incorporate the novel technologies and dynamics necessary to support the clean energy transition. The plan will contextualize existing efforts across the U.S. government, identify gaps or requirements for prioritization, and engage stakeholders across sectors, technology stacks, and jurisdictions to ensure national investments via the BIL, IRA, and Creating Helpful Incentives to Produce Semiconductors (CHIPS) & Science Act are cyber secure, resilient by design, and capable of supporting the novel operating circumstances of a clean energy ecosystem.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: CPO, NEC, OSTP

Completion Date: 2Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 4.4.3

Initiative Title: Build and refine training, tools, and support for engineers and technicians using cyber-informed engineering principles

Initiative Description

The Department of Energy will work with stakeholders to build on the National Cyber-Informed Engineering Strategy to advance the training, tools, and support for engineers and technicians to enable them to design, build, and operate operational technology and control systems that are secure- and resilient-by-design.

NCS Reference

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.

Responsible Agency: DOE

Contributing Entities: NIST

Completion Date: 4Q FY25

★ ★ ★ ★ ★ ★

Strategic Objective 4.6: Develop a National Strategy to Strengthen Our Cyber Workforce

Initiative Number: 4.6.1

Initiative Title: Publish a National Cyber Workforce and Education Strategy and track its implementation

Initiative Description

The Office of the National Cyber Director will lead the development of the National Cyber Workforce and Education Strategy and will drive, coordinate, and report on initial stages of implementation of the strategy. ONCD will act as the central coordinator for nationally prioritized workforce and education initiatives.

NCS Reference

To address this challenge, ONCD will lead the development and oversee implementation of a National Cyber Workforce and Education Strategy.

Responsible Agency: ONCD

Completion Date: 2Q FY24

Pillar Five: Forge International Partnerships to Pursue Shared Goals

Strategic Objective 5.1: Build Coalitions to Counter Threats to Our Digital Ecosystem

Initiative Number: 5.1.1

Initiative Title: Create interagency teams for regional cyber collaboration and coordination

Initiative Description

The Department of State will develop department staff knowledge and skills related to cyberspace and digital policy that can be used to establish and strengthen country and regional interagency cyber teams to facilitate coordination with partner nations.

NCS Reference

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.

Responsible Agency: State

Contributing Entities: Commerce, DHS, DOJ, CISA, FBI, USAID

Completion Date: 1Q FY25

★ ★ ★ ★ ★ ★

Initiative Number: 5.1.2

Initiative Title: Publish an International Cyberspace and Digital Policy Strategy

Initiative Description

In accordance with the Fiscal Year 2023 National Defense Authorization Act (Public Law 117-263, Section 9503), the Department of State will publish an International Cyberspace and Digital Policy Strategy that incorporates bilateral and multilateral activities.

NCS Reference

...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.

Responsible Agency: State

Contributing Entities: OMB, ONCD

Completion Date: 1Q FY24

Initiative Number: 5.1.3

Initiative Title: Strengthen Federal law enforcement collaboration mechanisms with allies and partners

Initiative Description

The FBI will develop or expand mechanisms to ensure coordination with allies and partners in efforts to increase the volume and speed of international law enforcements disruption campaigns against cybercriminals and nation-state adversaries, and associated enablers (e.g., money launderers).

NCS Reference

The United States will work with its allies and partners to develop new collaborative law enforcement mechanisms for the digital age: (1) The United States and international counterparts can advance common cybersecurity interests by sharing cyber threat information…and coordinating policy and incident response activities; and (2) the United States will… collaboratively disrupt transnational criminals and other malicious cyber actors, build the capacity of our international allies and partners,...and punish those that engage in disruptive, destructive, or destabilizing malicious cyber activity.

Responsible Agency: FBI

Contributing Entities: DHS, DOD, DOJ, State, Treasury

Completion Date: 4Q FY25

★ ★ ★ ★ ★ ★

Initiative Number: 5.1.4

Initiative Title: Regional cyber hubs study

Initiative Description

The Office of the National Cyber Director will commission a study on the European Cybercrime Centre to inform the development of future cyber hubs.

NCS Reference

To extend this model, we will need to support efforts to build effective hubs with partners in other regions.

Responsible Agency: ONCD

Contributing Entities: DOJ, State, FBI

Completion Date: 4Q FY24

Strategic Objective 5.2: Strengthen International Partner Capacity

Initiative Number: 5.2.1

Initiative Title: Strengthen international partners' cyber capacity

Initiative Description

The Department of State and other relevant interagency stakeholders will leverage the existing Interagency Cyber Capacity Building Working Group to assess the current global and policy trends in cyberspace; review the progress and investments made to date with the community of U.S. government implementers to achieve U.S. cyber goals, to include the six lines of effort in Strategic Objective 5.2; and prioritize future international capacity building assistance.

NCS Reference

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 support our shared interests in cyberspace by adhering to international law and reinforcing norms of responsible state behavior.

Responsible Agency: State

Contributing Entities: Commerce, DHS, DOD, DOE, DOJ, Treasury, CISA, FBI, USAID

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 5.2.2

Initiative Title: Expand international partners' cyber capacity through operational law enforcement collaboration

Initiative Description

Federal law enforcement will increase operational collaboration with international peer and near-peer law enforcement partners, thereby increasing such partners' capacity to disrupt the most significant cyber threats at a speed and scale that matches U.S. law enforcement's own goals.

NCS Reference

We must enable our allies and partners to…build law enforcement capacity and effectiveness through operational collaboration…

Responsible Agency: DOJ

Contributing Entities: State, FBI, HSI, USSS

Completion Date: 4Q FY26

Strategic Objective 5.3: Expand U.S. Ability to Assist Allies and Partners

Initiative Number: 5.3.1

Initiative Title: Establish flexible foreign assistance mechanisms to provide cyber incident response support quickly

Initiative Description

The Department of State will identify or develop a flexible and rapid foreign assistance mechanism to provide cyber incident response support.

NCS Reference

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.

Responsible Agency: State

Contributing Entities: DHS, DOD, FBI, USAID

Completion Date: 1Q FY24

★ ★ ★ ★ ★ ★

Strategic Objective 5.4: Build Coalitions to Reinforce Global Norms of Responsible State Behavior

Initiative Number: 5.4.1

Initiative Title: Hold irresponsible states accountable when they fail to uphold their commitments

Initiative Description

The Department of State will work through the Open-Ended Working Group to advance the framework of responsible state behavior in cyberspace and strengthen the coalition of states willing to hold malign actors responsible.

NCS Reference

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.

Responsible Agency: State

Contributing Entities: DOD, DOJ, FBI

Completion Date: 4Q FY25

★ ★ ★ ★ ★ ★

Strategic Objective 5.5: Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services

Initiative Number: 5.5.1

Initiative Title: Promote the development of secure and trustworthy information and communication technology (ICT) networks and services

Initiative Description

The Department of State will work with allies and partners through International Technology Security and Innovation funding to advance international adoption of policies and regulatory frameworks for secure ICT ecosystems.

NCS Reference

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.

Responsible Agency: State

Contributing Entities: Commerce, DHS, NSC, ONCD, USTR

Completion Date: 2Q FY24

Initiative Number: 5.5.2

Initiative Title: Promote a more diverse and resilient supply chain of trustworthy information and communication (ICT) vendors

Initiative Description

The Department of State will expand work with allies and partners through International Technology Security and Innovation funding to promote the development and deployment of open and interoperable network architectures.

NCS Reference

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.

Responsible Agency: State

Contributing Entities: Commerce, DFC, EXIM, USAID, USTDA

Completion Date: 2Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 5.5.3

Initiative Title: Begin administering the Public Wireless Supply Chain Innovation Fund (PWSCIF)

Initiative Description

The National Telecommunications and Information Administration (NTIA) will catalyze the development and adoption of open, interoperable, and standards-based networks through administration of the 10-year, $1,500,000,000 PWSCIF. Through this program, NTIA will strengthen supply chain resiliency, drive innovation, and foster competition. The first wave of funding, which NTIA intends to begin awarding in August 2023, will help drive testing and evaluation capabilities for open and interoperable networks and develop methodologies to test and evaluate performance, security, and efficiency of open and interoperable networks.

NCS Reference

...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.

Responsible Agency: NTIA

Contributing Entities: DHS, DOD, ODNI, FCC, NIST

Completion Date: 4Q FY23

Initiative Number: 5.5.4

Initiative Title: Promulgate and amplify Cybersecurity Supply Chain Risk Management (C-SCRM) key practices across and within critical infrastructure sectors

Initiative Description

Increase trust in foreign suppliers through the promulgation and amplification of C-SCRM best practices at home and abroad though a Software Supply Chain Security National Cybersecurity Center of Excellence Project.

NCS Reference

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.

Responsible Agency: NIST

Completion Date: 2Q FY25

Implementation-wide Initiatives

Implementation 6.1: Assessing Effectiveness

Initiative Number: 6.1.1

Initiative Title: Report progress and effectiveness on implementing the National Cybersecurity Strategy

Initiative Description

The Office of the National Cyber Director will assess the effectiveness of this strategy, associated policy, and follow-on actions and provide the first annual report to the President, the Assistant to the President for National Security Affairs, and Congress.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: OMB

Completion Date: 3Q FY24

Initiative Number: 6.1.2

Initiative Title: Apply lessons learned to the National Cybersecurity Strategy implementation

Initiative Description

The Office of the National Cyber Director will identify key lessons learned from cyber incidents and apply them to the implementation plan of the National Cybersecurity Strategy. ONCD will work with the appropriate departments and agencies to review Cyber Safety Review Board (CSRB) recommendations and determine if ONCD should incorporate them into broader NCS implementation plan efforts.

NCS Reference

The Federal Government will prioritize capturing lessons learned from cyber incidents and apply those lessons in the implementation of this strategy...Federal agencies also will promote and amplify CSRB recommendations that are directed to network defenders in the private sector.

Responsible Agency: ONCD

Contributing Entities: DHS, DOD, DOJ, CISA, FBI, NSA, OMB

Completion Date: 2Q FY24

★ ★ ★ ★ ★ ★

Initiative Number: 6.1.3

Initiative Title: Align budgetary guidance with National Cybersecurity Strategy implementation

Initiative Description

The Office of the National Cyber Director and OMB will ensure that their jointly issued annual guidance on cybersecurity budget priorities to departments aligns with the National Cybersecurity Strategy and will work with Congress to fund cybersecurity activities to keep pace with the speed of change inherent within the cyber ecosystem.

NCS Reference

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.

Responsible Agency: ONCD

Contributing Entities: OMB

Completion Date: 4Q FY23

Acronyms Used

3Q	Third Quarter
AML	Anti-Money Laundering
BIL	Bipartisan Infrastructure Law
BGP	Border Gateway Protocol
CFT	Countering the Financing of Terrorism
CIA	Central Intelligence Agency
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CISA	Cybersecurity and Infrastructure Security Agency
CPO	White House Climate Policy Office
C-SCRM	Cybersecurity Supply Chain Risk Management
CSF	Cybersecurity Framework
CSRB	Cyber Safety Review Board
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
EO	Executive Order
EOP	Executive Office of the President
EXIM	Export-Import Bank of the United States
FAR	Federal Acquisition Regulation
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCEB	Federal Civilian Executive Branch
FY	Fiscal Year
IaaS	Infrastructure-as-a-Service
ICTS	Information and Communications Technology and Services
IoT	Internet of Things
IPEF	Indo-Pacific Economic Framework for Prosperity
IPv6	Internet Protocol version 6
IRA	Inflation Reduction Act

ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JRTF	Joint Ransomware Task Force (co-chaired by CISA and FBI; membership includes DHS, DOD, DOJ, ODNI, State, Treasury, CIA, NSA and USSS)
NCIJTF	National Cyber Investigative Joint Task Force (Led by the FBI, membership includes CIA, CISA, NSA, USSS)
NCIRP	National Cyber Incident Response Plan
NCS	National Cybersecurity Strategy
NEC	National Economic Council
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSM	National Security Memorandum
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
ODNI	Office of the Director for National Intelligence
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OS3I	Open-Source Software Security Initiative
OSTP	Office of Science and Technology Policy
R&D	Research and Development
SBOM	Software Bill of Materials
SLTT	State, local, Tribal, and territorial
SRMA	Sector Risk Management Agency
State	Department of State
TMF	Technology Modernization Fund
TTC	Trade and Technology Council
Treasury	Department of the Treasury
USAID	United States Agency for International Development
USSS	United States Secret Service
USTR	United States Trade Representative

In Memory of Samantha Jennings-Jones

Samantha "Sam" Jennings-Jones worked in the Office of the National Cyber Director and was the first staffer assigned to work on the National Cybersecurity Strategy Implementation Plan. Through her dedication to public service and the cybersecurity mission, she built the initial list of initiatives that flowed from the Strategy and developed the template for this novel document.

Tragically, Samantha died after being struck by a car on March 30, 2023, four weeks to the day after the release of the strategy and before she could see the impact of her efforts.

This Implementation Plan is dedicated to her memory.