THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC REPORT TO THE PRESIDENT

Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem

February 21, 2023

Contents

Executive Summary ES-1

REPORT FOCUS AND SCOPE ES-1

SUMMARY OF KEY FINDINGS ES-1

SUMMARY OF RECOMMENDATIONS ES-3

1. Introduction 1

1.1. BACKGROUND 1

1.2. EARLIER PHASES AND THEIR RELATIONSHIP WITH PHASE IV 1

1.2.1. Software Assurance in the Information and Communications Technology and Services Supply Chain 2

1.2.2. Zero Trust and Trusted Identity Management 2

1.2.3. Information Technology and Operational Technology Convergence 2

1.3. PERSISTENT CHALLENGES IN ESTABLISHING SECURITY REQUIREMENTS FOR ICT 2

1.4. PERSISTENT CHALLENGES IN SECURITY ASSURANCE FOR ICT 3

2. Key Findings 5

2.1. URGENT ACTION IS NEEDED TO ADDRESS CYBER THREATS 5

2.2. PRESIDENTIAL ACTION CREATES RESULTS 6

2.3. ADVANCING ADOPTION AND ASSURANCE OF SECURITY TECHNOLOGIES REQUIRES SUSTAINED EFFORTS 7

2.4. PROLIFERATING CYBERSECURITY REQUIREMENTS AND ASSURANCE PROGRAMS DIVERT RESOURCES 8

2.5. CONSENSUS STANDARDS ARE CRITICAL FOR ASSURANCE HARMONIZATION 12

2.6. COLLABORATION IMPROVES CYBERSECURITY 13

2.7. CYBERSECURITY IS A SHARED RESPONSIBILITY 14

3. Recommendations 16

3.1. RECOMMENDATIONS BASED ON REVIEW OF PHASES I THROUGH III 16

3.1.1. Recommendation: Create and improve transparent procurement language encouraging vendor security best practices. 16

3.1.2. Recommendation: Enhance CISA's Continuous Diagnostics and Mitigation (CDM) Program. 17

3.1.3. Recommendation: Maximize automation and reuse of evidence in federal compliance with FISMA. 18

3.2. FEDERAL GOVERNMENT CYBERSECURITY HARMONIZATION EXPERTISE 19

3.2.1. Recommendation: Establish a government office with a primary mission of driving regulatory harmonization. 19

3.3. CYBERSECURITY REGULATORY HARMONIZATION POLICY AND PROCESS 22

3.3.1. Recommendation: Create policies and processes to encourage regulatory harmonization. 22

3.4. FEDERAL GOVERNMENT CYBERSECURITY REQUIREMENT HARMONIZATION AND CONSENSUS STANDARDS 24

3.4.1. Recommendation: Create policies and processes to encourage federal government cybersecurity requirement harmonization and drive consensus standards development. 24

3.5. POST QUANTUM CRYPTOGRAPHY 26
3.5.1. Recommendation: Advance the adoption of Post Quantum Cryptography (PQC). 26
4. Conclusion 27
Appendix A. Earlier Study Phases Summaries A-1
A.1. PHASE I: SOFTWARE ASSURANCE IN THE INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) AND SERVICES SUPPLY CHAIN A-1
A.1.1. Software Assurance A-1
A.1.2. Stakeholders A-3
A.1.3. External Factors A-4
A.2. PHASE II: ZERO TRUST AND TRUSTED IDENTITY MANAGEMENT A-4
A.3. PHASE III: INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY CONVERGENCE A-5
Appendix B. Membership and Participants B-1
Appendix C. Acronyms C-1
Appendix D. Definitions D-1
Appendix E. Bibliography E-1

Figures and Tables

Figure 1: Advancing Cybersecurity Requirements [2021-2022] 9
Table 1: Compliance Offerings of Cloud Service Providers 11

Executive Summary

Report Focus and Scope

In May 2021, in the aftermath of a series of significant cybersecurity incidents, the White House tasked the President's National Security Telecommunications Advisory Committee (NSTAC) with conducting a multi-phase study on "Enhancing Internet Resilience in 2021 and Beyond." The tasking directed NSTAC to focus on three key cybersecurity topics foundational to United States (U.S.) national security and emergency preparedness (NS/EP), producing these reports to the President:

> Phase I: Software Assurance in the Information and Communications Technology and Services Supply Chain.
>
> Phase II: Zero Trust and Trusted Identity Management.
>
> Phase III: Information Technology (IT) and Operational Technology (OT) Convergence.

The first three phases of the NSTAC tasking focused on developing recommendations to address each of these issues. This fourth and culminating phase not only refines and builds upon the key findings of phases I, II, and III, but also addresses challenges that organizations encounter in providing security assurance in response to increasing government security requirements to address cybersecurity risks. Security assurance can be defined as grounds for justified confidence that a security claim has been or will be achieved,[1] which is usually accomplished with an attestation by an organization that requirements have been fulfilled.[2] Security assurance encompasses two separate but interrelated overarching challenges relevant to the three prior phases: (1) how security requirements can best be defined, and (2) how organizations can best provide assurance that they are meeting those requirements. A more effective system for providing security assurance has the potential to incentivize greater implementation of software assurance, zero trust and identity management, OT security, as well as other cybersecurity improvements.

Summary of Key Findings

- **Urgent Action Is Needed to Address Cyber Threats.** Information and communications technology (ICT) systems are subject to continuous and expanding cyber threats. With some systems becoming obsolete, software components being increasingly reused, systems becoming more complex with more permeable boundaries, and IT and OT environments increasingly connected, defenders need to take urgent and sustained action to mitigate risks.

[1] "Security Assurance," National Institute of Standards and Technology (NIST), accessed January 4, 2023, https://csrc.nist.gov/glossary/term/security_assurance.

[2] "Attestation," NIST, accessed January 4, 2023, https://csrc.nist.gov/glossary/term/attestation.

- **Presidential Action Creates Results.** White House visibility into and prioritization of security issues facilitates increased interagency collaboration and improved public-private partnerships that can significantly advance cybersecurity outcomes.

- **Advancing Adoption and Assurance of Security Technologies Requires Sustained Efforts.** Improving approaches in software assurance, zero trust, information sharing, automation, machine-readable assurance artifacts, continuous diagnostics, and asset inventories provide opportunities to help producers and adopters of ICT technologies (including operational technologies) to improve security and resilience but require sustained effort to research, deploy and operationalize, especially in federal Departments and Agencies (hereinafter, "Agencies").

- **Proliferating Cybersecurity Requirements and Assurance Programs Divert Resources.** Growing concerns about cybersecurity risks have caused requirements and assurance programs to dramatically increase domestically and internationally, diverting resources from improving security to proving compliance with overlapping, redundant and/or inconsistent requirements, particularly for foundational ICT products that support multiple regulated sectors.

- **Consensus Standards Are Critical for Assurance Harmonization.** ICT standards for security requirements and assurance approaches developed with industry, regulators, and other experts collaborating across sectors and regions are reflective of global best practices. Alignment with consensus standards will deconflict, simplify, and align regionally developed compliance solutions so assurance activities can be done efficiently once and reused globally.

- **Collaboration Improves Cybersecurity.** Action by the U.S. government with industry creates more effective technical mechanisms for proving and communicating compliance with requirements to users and regulators. To this end, the U.S. government and industry could partner to better:

    - Focus on simplicity, consistency, and harmony in setting purchasing standards, thus making it easier for vendor communities to prove their products and services satisfy requirements;

    - Evaluate and adjust their own compliance programs to recognize and accept consensus standards and machine-readable records; and

    - Move towards compliance schemes that increase the use of automation and the reuse of compliance artifacts, and that use process- or framework-based evaluations versus point in time certifications.

- **Cybersecurity is a Shared Responsibility.** Workforce expertise and accountability for cybersecurity remain an ongoing challenge requiring the government and private sector to better fund cybersecurity education and training for all job roles; reinforce a culture that makes all stakeholders responsible for security; and encourage ICT providers to increase the use of secure defaults, adopt secure development methodologies, and actively employ risk mitigation measures for products during their lifecycle.

Summary of Recommendations

Recommendations based on Review of Phases I through III

1. **Create and improve transparent procurement language encouraging vendor security best practices.** The Cybersecurity and Information Security Agency (CISA), in consultation with private and public sector partners, should work with the General Services Administration (GSA) to draft core, universally applicable procurement language that clearly defines the government's requirements and preferences to help federal Agencies increasingly do the following, despite the work spanning multiple yearly budgeting cycles:

    - Require software to be developed and maintained according to current National Institute of Standards and Technology (NIST) supply chain risk management and software assurance guidance;

    - Prefer services provided by organizations that prioritize cybersecurity within their own enterprise environments by aligning with specifically articulated zero trust standards and cybersecurity best practices; and

    - Prefer OT products and services that support asset inventorying and align, where applicable, with zero trust principles and other cybersecurity best practices.

2. **Enhance CISA's Continuous Diagnostics and Mitigation (CDM) program.** The CDM[3] program includes inventorying hardware and software assets, scanning and managing vulnerabilities, and streamlining compliance with the Federal Information Security Management Act (FISMA) and other federal cybersecurity mandates and initiatives. In addition to aligning the CDM program with zero trust as recommended in the Phase II study, the CDM program should:

    - Incorporate OT technologies, particularly on IT/OT converged networks, by performing continuous inventorying of OT devices, software, systems, and assets;

    - Categorize in software inventories software provided by producers following the NIST Special Publication (SP) 800-218: Secure Software Development Framework (SSDF) to better inform risk-based security priorities;

    - Include scanning and discovery of internet-accessible applications; and

    - Provide continuous and dynamic asset mapping as part of CDM shared services as static data pulls will have limited utility in today's constantly evolving IT environment.

[3] "Continuous Diagnostics and Mitigation," Cybersecurity and Infrastructure Security Agency (CISA), accessed January 4, 2023, https://www.cisa.gov/cdm.

3. **Maximize automation and reuse of evidence in federal compliance with FISMA.** Federal shared services programs (examples include the Cybersecurity Quality Service Management Office (QSMO),[4] Cybersecurity Assessments,[5] Cybersecurity Training and Exercises,[6] High Value Asset Program,[7] National Cybersecurity Protection System Program,[8] Cyber Incident Response,[9] and the Trusted Internet Connections Program)[10] should work towards a consistent approach for assessing implementation of FISMA requirements. Special considerations should be given to software assurance and supply chain risk management, zero trust practices and OT security best practices, maximizing processes and technologies that leverage automation and enabling the reuse of baseline assurance evidence in higher risk contexts.

Federal Government Cybersecurity Harmonization Expertise

4. **Establish a government office with a primary mission of driving regulatory harmonization.** CISA should establish an office, the Office of Cybersecurity Regulatory Harmonization (OCRH),[11] with the primary mission of advancing the harmonization of cybersecurity requirements. The office's responsibilities should include: (1) establishing expertise on cybersecurity regulations across sectors; (2) creating resources that regulators can use to more easily develop cybersecurity requirements that leverage consensus standards where possible; and (3) providing technical assistance to regulators during the rulemaking process. OCRH would institutionalize and expand upon existing harmonization efforts, such as the Cyber Incident Reporting Council and the Cybersecurity Forum for Independent and Executive Branch Regulators. OCRH's first task should be to coordinate with NIST to publish a public report that catalogs existing cybersecurity requirements across sectors, analyzes how they align or diverge from consensus standards down to the control level, and identifies opportunities to drive harmonization.

Cybersecurity Regulatory Harmonization Policy and Process

5. **Create policies and processes to encourage regulatory harmonization.** The president should direct the following actions to drive cybersecurity regulatory harmonization:

---

[4] "Cybersecurity Quality Services Management Office (Cyber QSMO)," CISA, accessed January 4, 2023, https://www.cisa.gov/cyber-qsmo.

[5] "Cyber Assessments," CISA, accessed January 4, 2023, https://www.cisa.gov/cyber-assessments.

[6] "Cybersecurity Training and Exercises," CISA, accessed January 4, 2023, https://www.cisa.gov/cybersecurity-training-exercises.

[7] "High-Value Asset Program Management Office," CISA, accessed January 4, 2023, https://www.cisa.gov/hva-pmo.

[8] "National Cybersecurity Protection System," CISA, accessed January 4, 2023, https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

[9] "Cyber Incident Response," CISA, accessed January 4, 2023, https://www.cisa.gov/cyber-incident-response.

[10] "Trusted Internet Connections," CISA, accessed January 4, 2023, https://www.cisa.gov/tic.

[11] The Office of Cybersecurity Regulatory Harmonization is a suggested name provided to simplify subsequent references to the office in the report. The name of the office may change, but the function is critical.

- Agencies issuing a regulatory rulemaking that creates or modifies cybersecurity requirements should, to the greatest extent possible, align the requirements to consensus standards and OCRH-developed regulatory resources. An issuing Agency must document how each requirement aligns to consensus standards or CISA-developed regulatory resources.

- The issuing Agency shall provide an assessment to the Office of Information and Regulatory Affairs (OIRA) in the Office of Management Budget (OMB) describing how the cybersecurity requirements align to consensus standards and OCRH-developed regulatory resources or explaining how and why the requirements diverge.

- OCRH shall provide OIRA with an independent assessment of each regulatory rulemaking creating or modifying cybersecurity requirements, separate from other CISA comments, describing how well the requirements align to consensus standards and OCRH-developed regulatory resources and what opportunities exist to increase alignment or harmonization.

- OIRA shall coordinate with the Office of the National Cyber Director (ONCD) to resolve conflicts between the issuing Agency and OCRH prior to a rule being published in the Federal Register.

- Independent regulatory agencies should be encouraged to follow the alignment analysis and OCRH assessment requirements to advance the shared objective of cybersecurity regulatory harmonization.

Federal Government Cybersecurity Requirement Harmonization and Consensus Standards

6. **Create policies and processes to encourage federal government cybersecurity requirement harmonization and drive consensus standards development.** The president should direct Agencies to take the following actions to drive internal federal government cybersecurity requirement harmonization:

    - Agencies issuing federal government cybersecurity requirements shall align them to existing consensus standards or provide justification for why requirements diverge from existing consensus standards.

    - An issuing Agency creating a federal government cybersecurity requirement that diverges from existing consensus standards shall create and execute a strategy for developing a consensus standard in consultation with NIST.

    - Agencies issuing federal government cybersecurity requirements shall review them, and then update or reaffirm them, as needed, but at least every five years. If they do not align to

consensus standards when issued, the requirements shall be reviewed at least every two years to determine if they can be aligned to consensus standards.

- The Department of State and Department of Commerce, in coordination with the Department of Homeland Security (DHS), shall develop and execute a strategy to encourage more foreign government participation in the development and adoption of specific consensus standards.

- Agencies with responsibility for government testing and certification schemes for cybersecurity, such as the Federal Risk and Authorization Management Program (FedRAMP), should publish reports identifying how their certifications overlap with other existing certifications and identify what opportunities exist to recognize other certifications based on consensus standards or develop policies that enable them to accept evidence provided to auditors for the other certifications.

Post Quantum Cryptography

7. **Advance the adoption of Post Quantum Cryptography (PQC).** The president should direct CISA and NIST to form a large-scale partnership inclusive of the private sector, public sector, and academia focusing on transition to post quantum cryptography based on the *NIST Cryptographic Standards and Guidelines Development Process*[12] with the goal of speeding up the adoption and deployment of PQC. DHS and the Department of Commerce should encourage the adoption of post quantum cryptography in the public and private sectors by creating incentives to adopt PQC in federal systems and procurement, commercial ICT products, transport protocols, and underlying internet infrastructure.

[12] NIST, "NIST Interagency Report (NISTIR) 7977 - Cryptographic Standards and Guidelines Development Process," March 2016, https://csrc.nist.gov/publications/detail/nistir/7977/final.

1. Introduction

1.1. Background

Information and communications technology (ICT), including hardware, software, and network-connected devices, have transformed the way people live, and people are increasingly dependent on these systems in every aspect of their daily lives. They are essential not only to providing critical services such as power, water, and telecommunications, but also to supporting other important services touching all aspects of commercial, educational, and social life. At the same time, attacks against these systems have increased in frequency and sophistication, creating legitimate public concern about the confidentiality, integrity, and reliability of these systems. As a result, governments, businesses, and individuals all want ICT products to be more secure.

How ICT vendors make products more secure and how they demonstrate the products are more secure are separate but interrelated problems. The former is about how the developers and operators of ICT products must take the steps necessary to reduce vulnerabilities, make those products harder to penetrate, and enhance their resilience to cyber threats. The latter is about "assurance" – how do those responsible for security give confidence to others that products/services are reliably secure for their customers' needs?

Against this backdrop, the number of security requirements and security assurance programs have increased dramatically. This cacophony has a cost. While government Departments and Agencies (hereinafter, "Agencies") and private businesses have long noted a shortage of qualified security personnel, they have nonetheless created an environment in which valuable and limited resources must be spent to comply with overlapping and sometimes redundant or inconsistent regulatory regimes. To create a more meaningful and robust system, the U.S. government must streamline the way that security requirements are created, strengthen mechanisms for vendors to demonstrate compliance, and provide easier ways for vendors to convey their efforts to concerned parties.

1.2. Earlier Phases and their Relationship with Phase IV

This final fourth and capstone phase of the "Enhancing Internet Resilience (EIR) in 2021 and Beyond" study builds on the work of the prior three phases, which were published in the span of nearly a year.

Phase	Title	Publication Date
I	Software Assurance in the Information and Communications Technology and Services Supply Chain	Nov 2, 2021
II	Zero Trust and Trusted Identity Management	Feb 23, 2022
III	Information Technology and Operational Technology Convergence	Aug 23, 2022

The content in this section briefly describes the focus of the prior phases. Appendix A provides summaries, reiterates findings and recommendations, and includes noteworthy developments that occurred after they were published. Separately, this report includes new recommendations that inure benefits to all phases or involve using mechanisms suggested in prior phases to address emerging challenges of concern to the President's National Security Telecommunications Advisory Committee (NSTAC).

1.2.1. Software Assurance in the Information and Communications Technology and Services Supply Chain

NSTAC's Phase I report focuses on software assurance and the ICT and services supply chain. The issue is important because of software supply chain compromises that highlighted critical risks and the large-scale ramifications for industry and government. The study delivers a broad range of findings primarily based on increasing security during the software development process and improving software supply chain risk management practices.

1.2.2. Zero Trust and Trusted Identity Management

NSTAC's Phase II report focuses on zero trust and trusted identity management. Zero trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur and, therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified. Zero trust is not a single technology, but many cybersecurity technologies can help enable the implementation of zero trust security principles.

1.2.3. Information Technology and Operational Technology Convergence

NSTAC's Phase III report on the convergence of information technology (IT) and operational technology (OT) focuses on the key challenges of securing OT systems against threats that emerge from connecting OT and IT networks and includes recommendations to identify emerging approaches to increase OT resiliency, including adaptations of IT security approaches to address OT security challenges.

Many organizations have connected IT and OT systems to leverage data that is generated to drive greater efficiencies and provide better services. However, this interconnectivity has exposed OT systems, many of which have been in service for decades, to cyber threats against which they were not designed to defend. The NSTAC was tasked with developing recommendations to improve the security of converged IT and OT systems.

1.3. Persistent Challenges in Establishing Security Requirements for ICT

Streamlining security requirements for ICT requires overcoming three persistent challenges with existing risk management and compliance regimes: (1) the general-purpose application of many ICT products; (2) the historical legacy of sector-specific regulation; and (3) the time and resource-intensive processes that are generally relied upon for certification schemes.

Risk management theory recommends that the security level of an asset should be commensurate with the value of the asset. For example, a rare and valuable painting should be heavily protected at considerable cost,

while a low-value painting may warrant no protection and cost nothing to protect. The challenge with ICT assets, however, is that their value often varies based on the context in which they are used, and the same ICT product may be protecting a high- or low-value asset depending on how it is used. For example, a standard computer can be used for personal computing or can be deployed as an engineering workstation controlling critical processes within a water treatment plant. Since some ICT producers want to produce broadly used products at low cost and others may not envision their products being used in critical scenarios, they may develop their products without extensive security features. While all producers could in theory develop all ICT for high-value usage scenarios, that approach would drive up costs and stifle innovation for low-value usage scenarios. Notably, some ICT producers do serve highly regulated and/or security conscious customers and security is paramount for their products and services.

The second challenge relates to how governments historically have regulated industries around "verticals" or "sectors" (e.g., the financial sector, the healthcare sector, the information technology sector, the power sector, and/or the government sector), with each sector having separate requirements and regulators. As modern computing and the Internet transformed the economy, however, the world found that ICT products underpin every sector. For example, banks, hospitals, and the ICT sector itself all run on ICT products. This means the new world has a horizontal layer (ICT products) upon which all verticals (sectors) rely.

Regulatory authorities across sectors have recognized the reliance on cybersecurity and have extended their existing frameworks to cover it, causing multiple authorities to manage separate security assurance programs. While some programs and requirements leverage consensus standards, others are uniquely created to address risks at a national or local level. The result is that ICT producers are having to directly comply with or develop capabilities to help their customers comply with hundreds of requirements that are often distinct, overlapping, or sometimes inconsistent.

1.4. Persistent Challenges in Security Assurance for ICT

While streamlining security requirements is important, it will not address persistent challenges that ICT vendors face in demonstrating compliance with requirements. As ICT products are composed of hundreds of subparts, each involving several component manufacturers and operators, effective security assurance in the ecosystem requires addressing: (1) who is responsible for meeting security requirements; (2) how should they demonstrate compliance; and (3) how should their compliance be communicated.

One way to conceptualize addressing these challenges is "unit of manageability," a practical measure that puts responsibility on those capable of fulfilling it. For ICT products and services, this means that each producer or operator must be responsible for his/her share of security. The creator of code, for example, whether proprietary or open source, must adopt secure software development frameworks and incorporate the code of others only after applying appropriate risk mitigations. Similarly, the operator of a network must mitigate risk to adequately secure parts and services it uses, as well as mitigate security risks from its own contributions.

The challenge in practically implementing a system whereby each product or service provider is responsible for the security of his/her contribution is creating efficient and effective technical mechanisms that can

demonstrate implementation of security requirements and convey evidence that shows tangible results of implementing the security requirements. It is one thing to run a tool and claim that ninety percent of all machines have been patched; it is another to produce the output of that tool and demonstrate that ninety percent of machines have been patched. To the extent that development and operational tools are designed to produce usable evidence of compliance, compliance becomes that much easier to demonstrate. This is not to suggest that the output of every tool should be made publicly available. For example, clearly, some information might be sensitive and abused if made available to criminal elements. The key is to decide what is useful, what can be shared, how it can be shared, and how it should be protected– issues that are not uncommon in regulated environments.

In sum, the most effective way to ensure the security of a product is to require each component manufacturer to adhere to security standards, and those standards must be either communicated directly or transmitted via the supply chain. Similarly, compliance with those standards must be communicated directly back to users/regulators or channeled back up through the supply chain.

2. Key Findings

2.1. Urgent Action Is Needed to Address Cyber Threats

Finding: *ICT systems are subject to continuous and expanding cyber threats. With some systems becoming obsolete, software components being increasingly reused, systems becoming more complex with more permeable boundaries, and IT and OT environments increasingly connected, defenders need to take urgent and sustained action to mitigate risks.*

A consistent theme in the reports from the three prior study phases was the increasing cybersecurity risk contrasted with growing use and dependencies on ICT technologies and the implications for national security and emergency preparedness (NS/EP). Phase I cites examples of supply chain attacks (e.g., SUNSPOT[13] evidencing the compromise of a vendor build environment to insert malware) and includes suggestions to broaden security assurance activities during software development and maintenance and to reduce threats through increased software supply chain risk management. The importance of fast security update deployment was highlighted by an example of attackers using automation and cloud infrastructure to rapidly transition from newly publicized vulnerabilities to large scale attacks within hours.[14] Phase II examines the potential for the adoption of zero trust principles to meaningfully transform cybersecurity outcomes over the next decade and beyond as adoption matures. In addition to a spectrum of security activities, zero trust aptly involves assuming the network perimeter is breached and requires protections for important data be implemented as close to the data as possible with logging and monitoring. The approach improves detection of unauthorized activities and gives defenders better visibility into their networks, in part to activate recovery procedures when compromises do occur. In the context of the convergence IT and OT technologies, Phase III noted the significant efficiency benefits of connecting OT systems to enable remote management and monitoring, but also the security risks associated with connecting OT managed infrastructure to IT systems. The criticality of availability for OT systems means additional risk mitigation measures beyond those commonly used for IT systems (e.g., rapid patch deployment) are essential to prioritize for OT systems.

The early lessons on the start of hostilities in Ukraine in February 2022 showed destructive malware attacks in cyberspace can be used as a component of strategies to impair NS/EP through cyber activities. As a Microsoft report concludes, "the lessons from Ukraine call for a coordinated and comprehensive strategy to strengthen defenses against the full range of cyber destructive, espionage, and influence operations."[15]

---

[13] "SUNSPOT," MITRE ATT&CK, January 12, 2021, https://attack.mitre.org/software/S0562/.

[14] Microsoft, "HAFNIUM Targeting Exchange Servers with 0-day Exploits," March 2, 2021, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers.

[15] Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft (blog), June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

The need for defenders to take urgent and sustained action is most clearly stated in the conclusion of Phase II, which welcomes the short-term actions in the Federal Zero Trust Strategy[16] through 2024 and recognizes actions to institutionalize zero trust will be measured in decades, not years.[17] Phase I similarly recommends tasks to improve software assurance that will take years to accomplish. One of the key findings of Phase III is "The United States has the technology and the knowledge to secure these [OT] systems but has not prioritized the resources required to implement solutions"[18], indicating many organizations need to begin their journey to better secure OT systems.

2.2. Presidential Action Creates Results

Finding: *White House visibility into and prioritization of security issues facilitates increased interagency collaboration and improved public-private partnerships that can significantly advance cybersecurity outcomes.*

Presidential action has resulted in significant forward progress in addressing cybersecurity issues in the areas of software assurance, zero trust, and IT/OT convergence and it will continue to be critical moving forward.

The President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity,[19] issued on May 12, 2021, directed several actions that produced a meaningful advancement for both software assurance and zero trust. As a result of the EO, the National Institute of Standards and Technology (NIST), in collaboration with the public and private sectors in many cases, created a definition for critical software, published guidance outlining security measures for critical software, issued guidelines that recommend minimum standards for vendors' testing of their software source code, and published preliminary guidelines for enhancing software supply chain security, among other things.[20] The Administration also issued a strategy for Agencies to move to zero trust architectures and budget guidance to ensure that they align resources toward those goals.[21]

The President's National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems, issued July 28, 2021, has been important in bringing focus to and advancing efforts to address the cybersecurity issues around IT/OT convergence. The White House, the Cybersecurity and Infrastructure Security Agency (CISA), and Sector Risk Management Agencies (SRMA) have completed three industrial control

---

[16] Office of Management and Budget, Executive Office of the President, "M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[17] President's National Security Telecommunications Advisory Committee (NSTAC), "Report to the President on Zero Trust and Trusted Identity Management," February 2022, page 27, https://www.cisa.gov/nstac-publications.

[18] President's NSTAC, "Report to the President on Information Technology and Operational Technology Convergence," August 2022, Executive Summary page 3, https://www.cisa.gov/nstac-publications.

[19] The White House, "Executive Order (EO) 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[20] "Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order," NIST, accessed January 4, 2023, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity.

[21] The White House, "FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity," October 11, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/.

system cybersecurity sprints with electricity, pipeline, and water and wastewater industries and has started a fourth with the chemical sector. Each sprint consisted of high-level public-private partnerships to advance the cybersecurity of industrial control systems. The NSM also directed CISA to issue goals for control systems across critical infrastructure sectors, which CISA completed with the release of the Cross-Sector Cybersecurity Performance Goals[22] (CPGs) in October 2022.

2.3. Advancing Adoption and Assurance of Security Technologies Requires Sustained Efforts

Finding: *Improving approaches in software assurance, zero trust, information sharing, automation, machine-readable assurance artifacts, continuous diagnostics, and asset inventories provide opportunities to help producers and adopters of ICT technologies (including operational technologies) to improve security and resilience but require sustained effort to research, deploy and operationalize, especially in Agencies.*

EO 14028 elevated ICT industry interest in software assurance and zero trust by prioritizing its use by Agencies. Phases I and II of this study recognize that despite advancements in defining software assurance best practices, work to adapt traditional supply chain risk management methodologies to software, and zero trust guidance and maturity models being published, the actual proliferation of those practices will take significant time.

Phase I notes the dynamic nature of modern software development whereby organizations are continually innovating how to do software development including, but not limited to, the pervasive use of open source within commercial products. Software has also become highly collaborative with developers using the cloud to manage source code, perform builds, conduct testing, identify security mistakes and in some cases automate deployment. New models such as development and operations (DevOps) allow developers to examine running systems to monitor and diagnose production issues (with safeguards such as just in time access). The impact of those changing practices means no single software assurance framework can apply to every situation and continuous refinement in software assurance is needed to accommodate always changing business practices. EO 14028 has also encouraged software providers to include a software bill of materials (SBOM) with their products, but the sheer size of the SBOMs for complex products is going to require machine readable forms to practically analyze and compare efficiently.

For zero trust, implementing logging, and capabilities for monitoring how, when, and by whom data is accessed will improve an organization's ability individually to detect compromises but will be most impactful when information sharing across federal Agencies enables identification of an attack on one system to be communicated across the government and prevented elsewhere. For IT/OT convergence, continuous diagnostics and real-time asset inventories help defenders identify and remediate unintentional connections between IT and OT systems or external networks.

The technology and assurance communities agree that it is important to develop clear techniques to provide evidence of assurance during the procurement process. At the same time, evidence-based and data-driven approaches to assurance are taking hold, not only in software, but also in hardware. These research and

[22] "Cross-Sector Cybersecurity Performance Goals," CISA, accessed January 4, 2023, https://www.cisa.gov/cpg.

development topics are aligned with best practices and standards. While the evidence of completing security processes is typically considered in conjunction with procurement, novel approaches have been developed to provide such evidence in a machine-readable form. For example, NIST has developed areas of automated testing for some portions of the Federal Information Processing Standards (FIPS) security evaluation.[23]

As another example, consensus standards that can be used to store and exchange supply chain security compliance artifacts and attestations are in the early stages of development. Such standards might specify how to generate and store output generated when an organization implements practices in the Secure Software Development Framework (SSDF), better enabling independent verification as well as automated and continuous assurance. One example of an initiative to work on related standards is called Supply Chain Integrity, Transparency and Trust (SCITT).[24]

Each of the prior three phases recommend research and more importantly adoption of approaches to improve security and resilience. All recommend greater use of Agency procurement activities to increase adoption.

2.4. Proliferating Cybersecurity Requirements and Assurance Programs Divert Resources

Finding: *Growing concerns about cybersecurity risks have caused requirements and assurance programs to dramatically increase domestically and internationally, diverting resources from improving security to proving compliance to overlapping, redundant and/or inconsistent requirements, particularly for foundational ICT products that support multiple regulated sectors.*

Cybersecurity requirements are proliferating. From 2021 to 2022, for example, multiple jurisdictions worldwide responded to increased cybersecurity risks by updating or creating new cybersecurity requirements. As depicted in Figure 1 below, at least eleven international jurisdictions developed, updated, or implemented cross-sector or sector-specific cybersecurity requirements, two advanced cyber incident reporting requirements, and nine advanced both.[25][26] The United States itself took several major actions to create and update cybersecurity requirements, including issuing EO 14028, promulgating emergency security directives containing new cybersecurity requirements for pipelines and rail,[27] and passing the Cyber Incident Reporting for Critical

---

[23] "Automated Cryptographic Validation Testing," NIST, accessed January 4, 2023, https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing.

[24] Internet Engineering Task Force (IETF), "Supply Chain Integrity, Transparency, and Trust: An open collaboration space to incubate Internet-Drafts for the IETF focusing on a global initiative for securing end-to-end supply chains.," GitHub (Internet hosting service), accessed January 5, 2023, https://github.com/ietf-scitt?msclkid=020292bba6db11ec8569eadc629a068c.

[25] Microsoft, "Microsoft Digital Defense Report 2022," 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us.

[26] The countries comprising the European Union are counted as one jurisdiction for this figure because their inclusion was primarily based on the EU's efforts to updating the Network and Information Security Directive (NIS) during the timeframe.

[27] "Security Directives and Emergency Amendments," Transportation Security Administration, accessed January 4, 2023, https://www.tsa.gov/sd-and-ea.

Infrastructure Act of 2022 (CIRCIA),[28] which authorizes CISA to issue regulations to require cyber incident reporting from critical infrastructure operators.

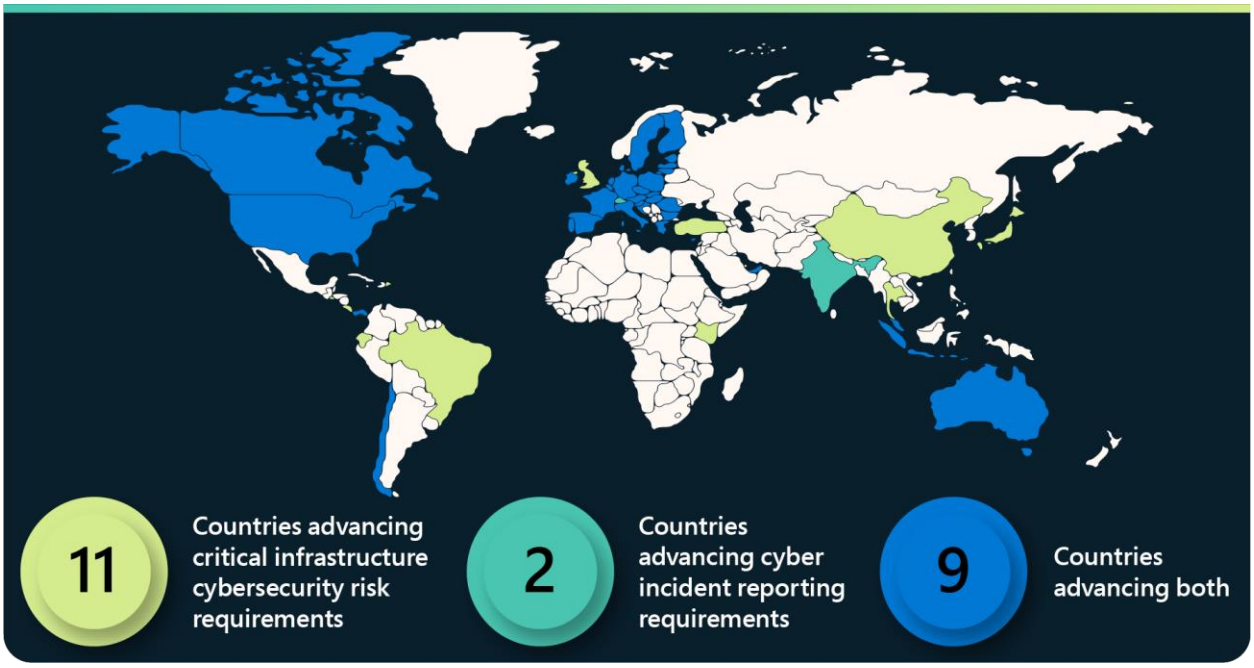

Figure 1: Advancing Cybersecurity Requirements [2021-2022]

These requirements often result in an increased need for organizations to prove that they are meeting their cybersecurity requirements through different assurance or certification programs, but these programs often end up diverging across sectors or countries resulting in additional cost without adding security benefit. The challenge is especially acute for cloud service providers and is representative of the challenge to the ICT industry.

Many different "types" of customers have introduced different certification schemes for cloud services over the past decade. There are public sector standards in many countries and even different schemes for different parts of the government, such as civilian, military, or intelligence. There are regulated sector schemes, and the schemes can differ for each sector across countries. There are consortia standards and formal standards, including International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standards. Some nations adopt ISO/IEC standards but then include changes specifically for their country.

Even though these schemes often have significant overlap in their requirements, each customer in each vertical bears the burden of proving compliance, with cloud providers having to support all such requirements for their customers. This increases costs without increasing security and may even force a provider to avoid smaller markets, particularly if its unique requirements are too stringent.

[28] "Cyber Incident Reporting for Critical Infrastructure Act of 2022," CISA, accessed January 5, 2023, https://www.cisa.gov/circia.

The table on the next page demonstrates the breadth of the challenge for cloud providers in managing many compliance programs globally. It merges the compliance offerings of multiple U.S. cloud providers[29,30,31,32] and organizes them into global, U.S. government, industry, and regional categories. A compliance offering in this table can be a certification, attestation, law, regulation, standard, or framework.

[29] "Amazon Web Services (AWS) Compliance Programs," AWS, accessed January 4, 2023, https://aws.amazon.com/compliance/programs/.

[30] "Compliance Offerings," Google Cloud, accessed January 5, 2023, https://cloud.google.com/security/compliance/offerings.

[31] "Azure Compliance Documentation," Microsoft, accessed January 5, 2023, https://learn.microsoft.com/en-us/azure/compliance/.

[32] "Oracle Cloud Compliance," Oracle, accessed January 4, 2023, https://www.oracle.com/corporate/cloud-compliance/#attestations.

Global	U.S. Government	Industry	Regional
• CIS Benchmark • CIS STAR Attestation • CSA STAR Certification • CSA STAR Self-Assessment • CyberGRX • CyberVadis • ISO 20000-1 • ISO 22301 • ISO 27001 • ISO 27017 • ISO 27018 • ISO 27701 • ISO 9001 • SOC 1 • SOC 2 • SOC 3 • WCAG 2.0 (ISO 40500)	• CJIS • CMMC • CNSSI 1253 • DFARS • DoD CC SRG • DoD IL2 • DoD IL4 • DoD IL5 • DoD IL6 • DoE 10 CFR Part 810 • EAR • FedRAMP • FISMA • FIPS 140-2 • ICD 503 • IRS 1075 • ITAR • JSIG • NIST 800-161 • NIST 800-171 • NIST 800-53 • NIST 800-63 • NIST CSF • Section 508 VPATs	**Automotive** • TISAX (Germany) **Education** • FERPA (US) **Energy** • NERC (US) **Financial Services** • 23 NYCRR 600 (US) • AFM + DNB (Netherlands) • AMF + ACPR (France) • APRA (Australia) • BaFin (Germany) • CFTC 1.31 (US) • CSSF (Luxembourg) • EBA (EU) • FCA + PRA (UK) • FFIEC (US) • FINMA (Switzerland) • FINTECH (Japan) • FINRA 4511 (US) • FISC (Japan) • FSA (Denmark) • GLBA (US) • KNF (Poland) • MAS + ABS (Singapore) • NBB + FSMA (Belgium) • OSFI (Canada) • OSPAR (Singapore) • PCI 3DS • PCI DSS Level 1 • RBI + IRDAI (India) • SEC 17a-4 (US) • SEC Regulation SCI (US) • Shared Assessments (US) • SOX (US) • TruSight **Healthcare and Life Sciences** • ASIP HDS (France) • GxP (FDA 21 CFR Part 11) • HIA (Canada, Alberta) • HIPAA (US) • HITRUST • MARS-E (US) • Medical Information Guidelines (Japan) • NEN 7510 (Netherlands) **Media and Entertainment** • CDSA • DPP (UK) • FACT (UK) • MPA **Telecommunications** • GSMA	**Americas** • Argentina PDPA • Brazil LGDP • Canada CCCS Assessment • Canada Privacy Laws • Canada Protected B • US CCPA **Asia Pacific** • Australia DTA HCF • Australia IRAP • Australia PDPA • China GB 18030:2005 • China DJCP (MLPS) • China ISO 20000 • China ISO 27001 • China ISO 27018 • China TRUCS/CCCPPF • China TCS • India MeitY • Japan APPI • Japan ISMAP • Japan CS Mark Gold • Japan My Number Act • Korea K-ISMS • Korea PIPA • Malaysia PDPA • New Zealand ISPS • New Zealand PDPA • Philippines PDPA • Singapore MTCS Level 3 • Singapore PDPA • Taiwan PDPA • Thailand PDPA **Europe and Middle East** • EU CISPE Code • EU EN 301 549 • EU ENISA IAF • EU GDPR • EU Model Clauses • EU-US Privacy Shield • Finland PiTuKri • Germany C5 • Germany IT–Grundschutz Workbook • Netherlands BIR 2012 • Portugal GNS • Spain ENS High • Spain LOPD • Spain CCN SPSTIC • UK NCSC Cloud Security Principles • UK Cyber Essentials Plus • UK G-Cloud • UK PASF **Middle East and Africa** • South Africa POPI • Qatar NIA • UAE DESC

Table 1: Compliance Offerings of Cloud Service Providers

2.5. Consensus Standards Are Critical for Assurance Harmonization

Finding: *ICT standards for security requirements and assurance approaches developed with industry, regulators, and other experts collaborating across sectors and regions are reflective of global best practices. Alignment with consensus standards will deconflict, simplify, and align regionally developed compliance solutions so assurance activities can be done efficiently once and reused globally.*

Today, ICT standards are largely developed through industry-driven, voluntary, consensus-based standards bodies (referred to as "consensus standards" in this report). To help ensure the continued independence and success of the industry-driven voluntary standards and existing specification development models, stakeholders and countries should participate in international standards development and adopt international standards rather than setting their own country or region-specific standards. This is particularly true for standards related to security assurance. If security assurance activities can be performed once and consumed multiple times without customization, it decreases the resources involved in security compliance and allows an increase in resources working on improving security.

Outcome-focused requirements provide assurance that a security goal is achieved without specifying the precise mechanisms used to achieve it, enabling practitioners to implement traditional or innovative techniques and technologies. Outcome-focused requirements can also be resilient to evolving threats because if a new threat compromises a traditional mechanism used to satisfy the requirement, alternatives can be used without needing to redefine the requirement. Evaluating how outcome-focused requirements are satisfied requires a more sophisticated evaluator and greater coordination amongst evaluators to ensure consistent interpretation of divergent solutions.

The U.S government and other stakeholders need to proactively support moving towards a more effective and efficient system that establishes basic outcome-focused security requirements that can be used across sectors while allowing for enhanced security requirements within certain sectors. Security requirements and effective security assurance need to be implemented using consensus standards. The security requirements and assurance approaches need to be developed with industry, regulators, and other experts collaborating across sectors and harmonizing those requirements with consensus standards. Participation across these groups of stakeholders can identify if existing standards support or satisfy the goal or risk associated with proposed requirements or when improvements to standards are necessary.

Despite the strength of consensus standards, there will be cases where they do not adequately mitigate risks that regulators or practitioners need to address. Particularly, as new technical practices emerge, the best practices should be codified by international standards, thus ensuring consistency across the information technology industry and across the globe. These standards may relate to any practice relevant to ensuring greater security including, but not limited to, training developers, using tools, and running tests. The key is that the standards focus on outcomes as opposed to the use of specific technologies. Such flexibility will allow innovation as development and operational practices, user behavior, and threat models change.

2.6. Collaboration Improves Cybersecurity

Finding: *Action by the U.S. government with industry creates more effective technical mechanisms for proving and communicating compliance with requirements to users and regulators. To this end, the U.S. government and industry could partner to better:*

- *Focus on simplicity, consistency, and harmony in setting purchasing standards, thus making it easier for vendor communities to prove their products and services satisfy requirements;*
- *Evaluate and adjust their own compliance programs to recognize and accept consensus standards and machine-readable records; and*
- *Move towards compliance schemes that increase the use of automation and the reuse of compliance artifacts, and that use process- or framework-based evaluations versus point in time certifications.*

Transparent procurement language for federal and industry technology adoption encourages vendors to implement and support security techniques and technologies. Similar public/private partnerships could be leveraged in the future to address urgent security challenges for the nation.

The more the government and industry have simplicity, consistency, and harmony in setting purchasing standards, the easier it is for the vendor community to satisfy them. Baseline security requirements can also benefit organizations that do not prioritize security because establishing a broadly implemented minimum security bar will improve the security of all users.

The U.S. government's approach to acquiring and using technology for its own needs influences and many times drives the:

- Available product options and versions because the U.S. government is a major purchaser of ICT; and
- Approach used by the private sector in business-to-business and business-to-consumer sales and by other governments since U.S. approaches are often emulated by others.

While the U.S. government is a positive driver for improved security for both critical infrastructure and other products and services, it can also create uncertainty, place unnecessary burdens on industry resources, deter innovative approaches, and lower the quality of rules and guidance through duplicative and competing efforts to put requirements in place.

To address cybersecurity challenges, multiple parts of the U.S. government sometimes use similar processes or requirements, such as cybersecurity controls for enterprises and information systems, cybersecurity supply chain risk management, and secure software development practices. However, Agencies do not always communicate with one another when developing and implementing these processes and requirements, creating silos. This can result in disparate requirements, guidance, and programs without coordination across the government, and industry sometimes lacks insight regarding the relationship between the initiatives. And, perhaps most

importantly, the processes depend on getting stakeholder input to be effective and are competing for industry attention and engagement.

Industry and other non-government organization expertise is needed to contribute to effective cybersecurity requirements and programs. Uncoordinated approaches (which have accelerated in the past couple of years):

- Limit the ability of industry and other stakeholders to fully review, contribute to, and engage in each of the proposed approaches; and
- Make the U.S. government's approach unclear and outcomes unpredictable, as the different government actors strive to accomplish their similar missions independently.

Duplicative or similar programs require unnecessary effort and take resources away from industry to better secure products, services, and networks.

Many ICT providers serve a global marketplace. Automation and reuse are key solutions to satisfying similar requirements internationally. The more organizations can automate assurance activities the more reliable and consistently they can fulfill them.

For modern ICT products that are updated on a continual basis (e.g., to address new attack techniques or vulnerabilities discovered), being able to certify processes used to update and operate ICT products versus undergoing a new evaluation for every change offers significant cost savings and increases the speed that security updates can be developed and deployed.

2.7. Cybersecurity is a Shared Responsibility

Finding: *Workforce expertise and accountability for cybersecurity remains an ongoing challenge requiring the government and private sector to better fund cybersecurity education and training for all job roles; reinforce a culture that makes all stakeholders responsible for security; and encourage ICT providers to increase the use of secure defaults, adopt secure development methodologies, and actively employ risk mitigation measures for products during their lifecycle.*

Threats exist during ICT product design, development, procurement, deployment, operations, and decommissioning. In each of the three earlier phase reports, they focus on the skills gap and recommend improving educational curriculum, materials, and guidance, building experience with practical application, building industry capacity by driving federal adoption, and tying security to procurement. Recommendations also include suggestions for recruiting people, raising awareness, and increasing international cooperation to address the shortage of skilled cybersecurity professionals and increase the cybersecurity knowledge level of technology

users and adopters. In addition, Phase III recommends cataloging and assessing the efficacy of OT workforce development efforts.[33]

Similar to the way EO 14028 created timelines for action by Agencies in adoption of software assurance, software supply chain risk management, and zero trust milestones and information sharing, Phase III recommends the Office of Management and Budget (OMB) work with CISA to develop key IT/OT convergence cybersecurity performance indicators and implementation timelines. Once in place, OMB should hold Agency heads accountable for achieving the indicators and timelines and using them to drive annual cybersecurity budget development.[34] The intent of this recommendation is to ensure that Agency heads assign responsibilities for OT security appropriately throughout their organizations to measurably reduce OT security risk.

All these efforts are intended to empower all stakeholders throughout organizations with better motivation, security training, and resourcing to address cybersecurity risks in practice across the breadth of ICT products and their lifecycle.

[33] President's NSTAC, "Report to the President on Information Technology and Operational Technology Convergence," August 2022, page 7, https://www.cisa.gov/nstac-publications.

[34] President's NSTAC, "Report to the President on Information Technology and Operational Technology Convergence," August 2022, page 5, https://www.cisa.gov/nstac-publications.

3. Recommendations

3.1. Recommendations based on Review of Phases I through III

3.1.1. Recommendation: Create and improve transparent procurement language encouraging vendor security best practices.

CISA, in consultation with private and public sector partners, should work with the General Services Administration (GSA) to draft core, universally applicable procurement language that clearly defines the government's requirements and preferences to help federal Agencies increasingly do the following, despite the work spanning multiple yearly budgeting cycles:

- *Require software to be developed and maintained according to current NIST supply chain risk management and software assurance guidance;*
- *Prefer services provided by organizations that prioritize cybersecurity within their own enterprise environments by aligning with specifically articulated zero trust standards and cybersecurity best practices; and*
- *Prefer OT products and services that support asset inventorying and align, where applicable, with zero trust principles and other cybersecurity best practices.*

EO 14028 advanced software assurance and supply chain risk management guidance with the publication of (a) NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities[35], (b) NIST 800-161 Rev 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations[36] and (c) evolving guidance on NIST's dedicated EO 14028 web-based portal.[37] Consistent with EO 14028, OMB has published memorandum M-21-30 on "Protecting Critical Software Through Enhanced Security Measures," [38] with the initial phase including standalone critical software and subsequent phases including software components used in OT. Also, OMB published memorandum M-22-18 on "Enhancing the Security of the Software Supply Chain through secure Software

[35] Murugiah Souppaya, Karen Scarfone, and Donna Dodson, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," NIST, February 2022, https://csrc.nist.gov/publications/detail/sp/800-218/final.

[36] Jon Boyens et al., "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," NIST, May 2022, https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final.

[37] "Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order," NIST, accessed January 4, 2023, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity.

[38] Office of Management and Budget, Executive Office of the President, "M-21-30: Protecting Critical Software Through Enhanced Security Measures," August 10, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf.

Development Practices"[39] to require Agencies to obtain self-attestation from software producers asserting that they follow the NIST guidance, initially for critical software and later all software.

Section 4.4 of the Phase II study recommends developing federal procurement preferences for organizations that prioritize cybersecurity within their own enterprise environments by aligning with specifically articulated zero trust standards and best practices. Section 1.1.2 of the Phase III study recommends CISA work with GSA to require inclusion of risk-informed cybersecurity capabilities in procurement vehicles for the federal government by developing enhanced OT-specific cybersecurity procurement language and requiring it for all federal OT procurement. It also recommends that there should be a mechanism for both private sector consumers and public sector agencies to provide feedback and lessons learned to improve the procurement language.

Per OMB M-21-30 and M-22-18, software assurance and supply chain risk management procurement requirements start with critical software and new products and apply over time to all software, including existing software that is modified by major version changes. If current software vendors to Agencies are unable to fully comply, Agencies are likely to require multiple years to transition to software available from compliant vendors. Similarly, as Phase II notes, the long-term horizon required to achieve zero trust maturity requires more flexible budgeting options that can support multi-year funding. Phase III notes that while a zero trust architecture may raise the bar for cybersecurity, it can be extremely difficult to implement in OT environments, which include both legacy and new equipment. Therefore, model procurement language should assist Agencies in budgeting more difficult cybersecurity improvements over multiple years.

The promise of vendors retaining eligibility to appear on federal supply schedules, federal government-wide acquisition contracts, and blanket purchase agreements would be a powerful driver of cybersecurity best practices.

3.1.2. Recommendation: Enhance CISA's Continuous Diagnostics and Mitigation (CDM) Program.

The CDM[40] program includes inventorying hardware and software assets, scanning and managing vulnerabilities, and streamlining compliance with the Federal Information Security Management Act (FISMA) and other federal cybersecurity mandates and initiatives. In addition to aligning the CDM program with zero trust as recommended in the Phase II study, the CDM program should:

- *Incorporate OT technologies, particularly on IT/OT converged networks, by performing continuous inventorying of OT devices, software, systems, and assets;*
- *Categorize in software inventories software provided by producers following the NIST SP 800-218: Secure Software Development Framework (SSDF) to better inform risk-based security priorities;*

[39] Office of Management and Budget, Executive Office of the President, "M-22-18: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," September 14, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

[40] "Continuous Diagnostics and Mitigation," CISA, accessed January 4, 2023, https://www.cisa.gov/cdm.

- *Include scanning and discovery of internet accessible applications; and*
- *Provide continuous and dynamic asset mapping as part of CDM shared services as static data pulls will have limited utility in today's constantly evolving IT environment.*

The Phase II study specifically identifies the value of aligning the CDM program with zero trust, but the program also could be leveraged for gathering accurate software and OT asset inventory, managing the distribution of software patches (with appropriate verification prior to deployment in OT environments). More software patches should be forthcoming with new federal requirements for software suppliers to attest to using the SSDF and implementing coordinated vulnerability disclosure policies.

Section 1.1.6 of the Phase III study notes the importance of hiring external parties to assess the risk of internet-facing assets or utilizing external attack surface management tools to automate the process as part of organizational security programs. Per Binding Operational Directive (BOD) 23-01[41], federal civilian executive branch Agencies operating information technology systems are required to maintain an up-to-date inventory of networked assets (including IT and OT) and identify software vulnerabilities by April 3, 2023.

3.1.3. Recommendation: Maximize automation and reuse of evidence in federal compliance with FISMA.

Federal shared services programs (examples include the Cybersecurity Quality Service Management Office (QSMO),[42] Cybersecurity Assessments,[43] Cybersecurity Training and Exercises,[44] High-Value Asset Program,[45] National Cybersecurity Protection System Program,[46] Cyber Incident Response,[47] and the Trusted Internet Connections Program)[48] should work towards a consistent approach for assessing implementation of FISMA requirements. Special considerations should be given to software assurance and supply chain risk management, zero trust practices and OT security best practices, maximizing processes and technologies that leverage automation and enabling the reuse of baseline assurance evidence in higher risk contexts.

Section 3.3.2 of the Phase I study recommends public sector IT deployment and operations functions should invest in artificial intelligence and automation to improve efficiency and efficacy of software assurance functions. Section 1.3(b)(i) of the Phase I study also recommends increasing efficiencies for security assurance, automation, and analysis for threat modeling. Section 3.2.2 of the Phase II report recommends using the shared

---

[41] CISA, "Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks," October 3, 2022, https://www.cisa.gov/binding-operational-directive-23-01.

[42] "Cybersecurity Quality Services Management Office (Cyber QSMO)," CISA, accessed January 4, 2023, https://www.cisa.gov/cyber-qsmo.

[43] "Cyber Assessments," CISA, accessed January 4, 2023, https://www.cisa.gov/cyber-assessments.

[44] "Cybersecurity Training and Exercises," CISA, accessed January 4, 2023, https://www.cisa.gov/cybersecurity-training-exercises.

[45] "High-Value Asset Program Management Office," CISA, accessed January 4, 2023, https://www.cisa.gov/hva-pmo.

[46] "National Cybersecurity Protection System," CISA, accessed January 4, 2023, https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

[47] "Cyber Incident Response," CISA, accessed January 4, 2023, https://www.cisa.gov/cyber-incident-response.

[48] "Trusted Internet Connections," CISA, accessed January 4, 2023, https://www.cisa.gov/tic.

services above as vehicles for procuring technologies to enable zero trust outcomes. Finally, section 1.2 of the Phase III study recommends expanding CISA services into OT specifically for state, local, tribal, and territorial (SLTT) infrastructure and that CISA should work with SRMAs to co-develop cyber incident response and recovery playbooks. This includes funding any required shared hardware, software, and staff training to execute those playbooks in conjunction with DHS fly-away teams and SRMA staff.

3.2. Federal Government Cybersecurity Harmonization Expertise

3.2.1. Recommendation: Establish a government office with a primary mission of driving regulatory harmonization.

CISA should establish an office, the Office of Cybersecurity Regulatory Harmonization (OCRH),[49] with the primary mission of advancing the harmonization of cybersecurity requirements. The office's responsibilities should include: (1) establishing expertise on cybersecurity regulations across sectors, (2) creating resources that regulators can use to more easily develop cybersecurity requirements that leverage consensus standards where possible, and (3) providing technical assistance to regulators during the rulemaking process. OCRH would institutionalize and expand upon existing harmonization efforts, such as the Cyber Incident Reporting Council and the Cybersecurity Forum for Independent and Executive Branch Regulators. OCRH's first task should be to coordinate with NIST to publish a public report that catalogs existing cybersecurity requirements across sectors, analyzes how they align or diverge from consensus standards down to the control level, and identifies opportunities to drive harmonization.

A consistent challenge identified during Phase IV briefings and discussions was the lack of a shared understanding of the degree to which existing cybersecurity regulations diverge across sectors and what exactly it means for cybersecurity regulations to be harmonized. An opportunity exists for CISA to establish and resource an office with the primary mission of advancing cybersecurity regulatory harmonization and tasking it with studying existing regulations and developing resources that could define how to create harmonized regulations. While existing government forums, such as the Cyber Incident Reporting Council and the Cybersecurity Forum for Independent and Executive Branch Regulators, are trying to address these challenges to varying degrees, none of them have the required combination of mission, expertise, and resources that can address the scale of the challenge.

In 2022 President Biden signed CIRCIA into law,[50] which directed the Secretary of Homeland Security to establish the intergovernmental Cyber Incident Reporting Council (CIRC) to "coordinate, deconflict, and harmonize federal incident reporting requirements, including those issued through regulations."[51] It also directed the Secretary to submit a report to Congress that includes a list of duplicative federal cyber incident reporting requirements, a

[49] The Office of Cybersecurity Regulatory Harmonization is a suggested name provided to simplify subsequent references to the office in the report. The name of the office may change, but the function is critical.

[50] United States (U.S.) Congress, Consolidated Appropriations Act, 2022, March 15, 2022, https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[51] Ibid.

description of any challenges in harmonizing the requirements, any actions the director intends to take to facilitate harmonization, and any proposed legislative changes necessary to address duplicative reporting. While the council's work is important in addressing the acute challenge around cyber incident reporting harmonization, its limited focus on incident reporting precludes it from meaningfully addressing broader harmonization challenges on a sustained basis.

In 2022 the Biden Administration also announced the revitalization of the Cybersecurity Forum for Independent and Executive Branch Regulators (Forum), a federal interagency group that shares information and expertise to enhance the cybersecurity of America's critical infrastructure.[52] The Forum was initially launched in response to the issuance of EO 13636 in 2013,[53] which required Agencies with responsibility for regulating security of critical infrastructure to engage in a consultative process with DHS, OMB, and National Security Staff, but the Forum had mostly been inactive in recent years. The revitalized group identified its priority as harmonizing how the private sector and federal government implement cybersecurity controls, with an initial focus on the topics of cyber incident reporting and advancing cybersecurity goals identified in EO 14028, such as advancing multi-factor authentication or zero trust architecture.[54] While the Forum has the right mission and broad representation, it does not have dedicated staffing who can focus on developing in-depth expertise of regulatory requirements across sectors because most participants are engaged in the Forum in addition to their normally assigned responsibilities at their home agencies.

Establishing OCRH within CISA and providing it with dedicated staffing and resources would create an institutionalized source of in-depth cybersecurity regulatory expertise across sectors that does not currently exist within the federal government. OCRH should not supplant existing efforts but should work collaboratively with them and support them as an expert resource. To accomplish this, OCRH should first establish its expertise on cybersecurity regulations across sectors by publishing a public report that catalogs existing cybersecurity requirements across sectors, analyzes how they align or diverge from consensus standards down to the control level, and identifies opportunities to drive harmonization. The report's objectives would be similar to those of the CIRCIA report, but its scope would expand beyond cyber incident reporting. In preparing the report, OCRH should solicit input from sector-specific regulators by leveraging existing efforts such as the CIRC and the Forum, who could in turn use the final report to inform their future efforts. The report should be published publicly to develop a shared understanding of the challenges and solutions with regulated entities and the broader private sector, who could also help advance solutions.

One of goals for the report should be to examine what regulatory resources OCRH could create to assist regulators in drafting cybersecurity requirements in a more harmonized way. A recurring challenge that the subcommittee heard is that even though most regulations cite consensus standards as the basis for their

---

[52] Federal Communications Commission, "Chairwoman Rosenworcel to Lead Federal Interagency Cybersecurity Forum," February 3, 2022, https://www.fcc.gov/document/chairwoman-rosenworcel-lead-federal-interagency-cybersecurity-forum.

[53] U.S. Nuclear Regulatory Commission, "Press Release-14-068: Interagency Cybersecurity Forum Meets: NRC Chairman Allison Macfarlane Chairs Inaugural Meeting," October 15, 2014.

[54] Lamar Johnson, "FCC Interagency Cybersecurity Forum to Focus on Harmonizing Private-Public Cyber," *Meritalk*, April 11, 2022, https://www.meritalk.com/articles/fcc-interagency-cybersecurity-forum-to-focus-on-harmonizing-private-public-cyber/.

requirements, variations in implementations across regulators often result in divergent requirements. Developing regulatory resources that provide common language that could be used across sectors could address the challenge. OCRH-regulatory resources could serve a similar purpose to that of OMB Circular A-4, "Regulatory Analysis," which is designed to assist regulatory agencies in defining good regulatory analysis and standardizing measurement and reporting of the benefits and costs.[55] Regulators would ideally be motivated to use OCRH-developed regulatory resources if the resources make it easier to draft and communicate their requirements. Transition from existing regulatory language to language that aligns to any OCRH-developed regulatory resource would most likely occur slowly as regulations are updated.

Developing regulatory resources that are flexible enough for all regulators to use and can still establish a shared language for setting requirements will be challenging, but these resources should be able to build upon existing efforts based in consensus standards for cybersecurity risk management and requirements, such as the NIST Cybersecurity Framework (CSF), NIST SP 800-53,[56] and CISA's CPGs, among others.

The CSF, for example, provides a common taxonomy for describing cybersecurity posture,[57] but because its application is left to the implementing organization, it can be difficult for regulators to rely on its implementation alone as proof of appropriate cybersecurity risk management. CISA-developed regulatory resources could leverage the common taxonomy of the CSF and provide guidance in how regulators can best apply its use.

Similarly, SP 800-53 establishes a shared lexicon around security controls for systems and organizations, where controls are defined as "descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders."[58] SP 800-53 does not require any particular control usage for most organizations, however, leaving it to the implementing organizations to determine what controls to use. The exception to this is NIST SP 800-53B,[59] which establishes control baselines and tailoring guidance for those baselines for federal information systems and organizations, in accordance with OMB Circular A-130 and provisions of FISMA. CISA-developed regulatory resources could leverage the SP 800-53 lexicon as well as use the baselines and tailoring guidance from SP 800-53B.

---

[55] "Frequently Asked Questions," Reginfo.gov, accessed January 5, 2023, https://www.reginfo.gov/public/jsp/Utilities/faq.jsp#reg_rule.

[56] NIST, "SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," September 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[57] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," April 26, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[58] NIST, "SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," September 2020, page 252, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[59] NIST, "SP 800-53B: Control Baselines for Information Systems and Organizations," October 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

Last, CISA published the CPGs in 2022, which "are a prioritized subset of IT and OT cybersecurity practices aimed at meaningfully reducing risks to both [critical infrastructure] operations and to the American people."[60] CISA-developed regulatory resources could potentially incorporate CPGs as a way of creating a shared lexicon around some requirements although this would likely require consideration because the CPGs are a newer concept and are not intended to be comprehensive.

The committee chose CISA as the best place to establish the proposed office primarily because the responsibilities are well aligned with CISA's role as National Coordinator for critical infrastructure security and resilience, which includes ensuring a unified approach to cyber risk management as described in a DHS report[61] responding to Sec. 9002 of the 2021 National Defense Authorization Act. The proposed office is also consistent with CISA's preference for remaining non-regulatory since the office would act only in an advisory capacity in support of other federal government regulators. Because of the criticality of consensus standards in driving harmonization, however, OCRH should have a strong partnership with NIST and should coordinate closely with them when developing the public report or regulatory resources, which should have a strong basis in consensus standards.

3.3. Cybersecurity Regulatory Harmonization Policy and Process

3.3.1. Recommendation: Create policies and processes to encourage regulatory harmonization.

The president should direct the following actions to drive cybersecurity regulatory harmonization:

- *Agencies issuing a regulatory rulemaking that creates or modifies cybersecurity requirements should, to the greatest extent possible, align the requirements to consensus standards and OCRH-developed regulatory resources. An issuing Agency must document how each requirement aligns to consensus standards or CISA-developed regulatory resources.*

- *The issuing Agency shall provide an assessment to the Office of Information and Regulatory Affairs (OIRA) in OMB describing how the cybersecurity requirements align to consensus standards and OCRH-developed regulatory resources or explaining how and why the requirements diverge.*

- *OCRH shall provide OIRA with an independent assessment of each regulatory rulemaking creating or modifying cybersecurity requirements, separate from other CISA comments, describing how well the requirements align to consensus standards and OCRH-developed regulatory resources and what opportunities exist to increase alignment or harmonization.*

- *OIRA shall coordinate with the Office of the National Cyber Director (ONCD) to resolve conflicts between*

---

[60] CISA, "Cross-Sector Cybersecurity Performance Goals," 2022, https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.

[61] United States (U.S.) Congress, "Fiscal Year 2021 National Defense Authorization Act," November 12, 2021, https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf.

the issuing Agency and OCRH prior to a rule being published in the Federal Register.

- *Independent regulatory agencies should be encouraged to follow the alignment analysis and OCRH assessment requirements to advance the shared objective of cybersecurity regulatory harmonization.*

One challenge in improving regulatory harmonization that was identified was how to motivate multiple, disparate Agencies separately engaged in cybersecurity rulemaking to advance harmonization when they are most focused on the objectives of their individual rulemaking. EO 12866, "Regulatory Planning and Review,"[62] issued in 1993, provides a model for achieving this objective because it establishes processes to ensure that rulemaking complies with the EO's regulatory principles and the president's policies and priorities. Adapting this model to advance cybersecurity regulatory harmonization would also provide opportunities to encourage regulators to use the resources that OCRH develops in support of regulatory harmonization.

Consistent with EO 12866, the Executive Branch should explicitly establish cybersecurity regulatory harmonization as a regulatory principle and require that cybersecurity requirements in rulemaking align to consensus standards and OCRH-developed regulatory resources. Issuing Agencies should be required to document and explain how the cybersecurity requirements in their rulemaking align to consensus standards or OCRH-developed regulatory resources or explain when requirements need to diverge. This documentation and analysis requirement is similar to the EO 12866 requirement that issuing Agencies assess the potential costs and benefits of a regulatory action, a requirement supporting the regulatory principle that regulations be designed in a cost-effective manner. The issuing Agency should document alignment at the level of individual requirements and provide an overall analysis to facilitate the ability of others to understand and assess the alignment.

During the 90 days that EO 12866 already gives OIRA to review significant regulations and coordinate interagency Executive Branch review,[63] the OCRH should provide OIRA with an independent assessment explaining how well the rulemaking aligns to consensus standards and OCRH-developed regulatory resources and what opportunities exist to improve alignment. This will enable OIRA to benefit from the in-depth regulatory harmonization expertise of the OCRH before providing feedback to the issuing Agency. This regulatory harmonization assessment should be separate from other CISA feedback to OIRA on the rulemaking to ensure that harmonization issues are considered distinctly. Ideally the OCRH assessment requirement will prompt Agencies to engage OCRH early in the drafting process for advice and assistance.

If significant disagreements between OCRH and the issuing Agency occur regarding the alignment of the rulemaking, OIRA should follow existing EO 12866 conflict resolution processes with the additional inclusion of ONCD. EO 12866 already empowers the Administrator of OIRA to resolve conflicts between or among Agency heads or between OMB and any Agency. For cybersecurity rulemaking conflicts, the Administrator should coordinate with the National Cyber Director since the Director is the principal advisor to the president on

---

[62] Reginfo.gov, "Executive Order 12866 of September 30, 1993: Regulatory Planning and Review," October 4, 1993, https://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf.

[63] "Frequently Asked Questions," Reginfo.gov, accessed January 5, 2023, https://www.reginfo.gov/public/jsp/Utilities/faq.jsp#reg_rule.

cybersecurity policy and strategy.[64] This coordination is needed to take advantage of the expertise within ONCD, and because if the Administrator cannot resolve the conflict, EO 12866 requires that the conflict be resolved by the president, or by the vice president acting at the request of the president.

One challenge in adapting existing EO 12866 processes toward the goal of cybersecurity regulatory harmonization is that independent regulatory agencies, as defined in 44 U.S.C. 3502(10)[65], are excluded from the EO's regulatory review requirements, which means that independent agencies that issue cybersecurity regulations, such as the Federal Communications Commission, the Federal Trade Commission, or the Federal Reserve, would not be covered by the recommended processes. To address this challenge, the Executive Branch should at a minimum encourage independent regulatory agencies to follow the same cybersecurity regulatory harmonization processes, especially since such an approach will serve to both improve security and reduce development and operational costs. Independent agencies would still retain final decision making for the contents of their rulemaking but adhering to alignment analysis and OCRH assessment requirements could still help drive regulatory harmonization.

3.4. Federal Government Cybersecurity Requirement Harmonization and Consensus Standards

3.4.1. Recommendation: Create policies and processes to encourage federal government cybersecurity requirement harmonization and drive consensus standards development.

The president should direct Agencies to take the following actions to drive internal federal government cybersecurity requirement harmonization:

- *Agencies issuing federal government cybersecurity requirements shall align them to existing consensus standards or provide justification for why requirements diverge from existing consensus standards.*
- *An issuing Agency creating a federal government cybersecurity requirement that diverges from existing consensus standards shall create and execute a strategy for developing a consensus standard in consultation with NIST.*
- *Agencies issuing federal government cybersecurity requirements shall review them, and then update or reaffirm them, as needed, but at least every five years. If they do not align to consensus standards when issued, the requirements shall be reviewed at least every two years to determine if they can be aligned to consensus standards.*
- *The Department of State and Department of Commerce, in coordination with DHS, shall develop and execute a strategy to encourage more foreign government participation in the development and adoption of specific consensus standards.*

---

[64] "Office of the National Cyber Director," The White House, accessed January 5, 2023, https://www.whitehouse.gov/oncd/.

[65] "44 USC 3502: Definitions," U.S. House of Representatives, accessed January 5, 2023, https://uscode.house.gov/view.xhtml?req=(title:44%20section:3502%20edition:prelim).

- *Agencies with responsibility for government testing and certification schemes for cybersecurity, such as FedRAMP, should publish reports identifying how their certifications overlap with other existing certifications and identify what opportunities exist to recognize other certifications based on consensus standards or develop policies that enable them to accept evidence provided to auditors for the other certifications.*

The federal government issues cybersecurity requirements for federal Agencies that are not subject to EO 12866 policies and processes because they are not created via regulatory rulemaking. Because these requirements originate with multiple entities and take various forms, the White House should establish a separate policy requiring that federal government cybersecurity requirements also align to consensus standards to ensure that they are also being harmonized.

OMB Circular A-130, "Managing Information as a Strategic Resource" demonstrates the diversity of requirements that Agencies must adhere to and should be covered by the policy. It requires Agencies "implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, DHS, GSA, and the Office of Personnel Management. This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs)."[66]

Because situations might arise where Agencies identify a gap in existing consensus standards, requirements should be able to diverge from consensus standards if justified. However, in these situations, issuing Agencies should be required to consult with NIST to create a strategy for developing a consensus standard that would address the gap. Acting quickly to create and execute a strategy to fill the gap will drive better harmonization outcomes by more quickly producing standards that others can align to. Agencies should also be required to update and reaffirm their requirements at least every five years to ensure their relevance and alignment to consensus standards, which can shift over time. When issuing requirements that cannot initially be aligned to consensus standards, the review time frame should shrink to two years with the goal of aligning it to consensus standards at that time.

Because the challenge of harmonization is not limited to U.S. borders, the Department of State and Department of Commerce, in coordination with DHS, should also develop and execute a strategy to encourage more foreign government participation in the development and adoption of specific consensus standards. A strategy would prioritize both the standards needed to drive harmonization and which countries to prioritize working with based on their potential to facilitate the best economic and cybersecurity outcomes.

Last, Agencies responsible for government testing and certification schemes for cybersecurity should be required to publish a report identifying how their certifications overlap with other existing certifications, whether this overlap can be eliminated, and whether the same evidence can be used to obtain multiple certifications.

---

[66] The White House, "Circular No. A-130: Managing Information as a Strategic Resource," 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

Consistent with the finding earlier in the report that proliferating cloud cybersecurity certification schemes are a significant challenge, the government's FedRAMP certification is a good candidate for the first report.

Currently, cloud companies that want to sell to multiple types of customers or in different countries must navigate a patchwork of technical requirements that often must be assessed by different accredited third parties. The bases of accrediting third parties often differ between compliance schemes. Each scheme that requires a third-party assessor entails internal preparatory work for both compliance staff and product development teams and hiring an auditing firm to get through a lengthy process that can take six to eighteen months before a service can be certified. Such certifications have expiration dates and often need to be maintained and/or are subject to continuous monitoring. A company selling globally today may have to comply with more than a hundred such programs despite the significant overlap among them.

The U.S. government has an opportunity to demonstrate global leadership by acknowledging and publicizing this overlap and working towards aligning their programs with compliance schemes based on consensus standards. Other governments will likely be unwilling to compromise on their schemes if the U.S. is unwilling to take the first step. By leading on this issue, the U.S. government will set an example for other governments, support interoperability, lower cloud costs by reducing duplicative requirements, and promote and support world-wide adoption of technology following security best practices.

3.5. Post Quantum Cryptography

3.5.1. Recommendation: Advance the adoption of Post Quantum Cryptography (PQC).

The president should direct CISA and NIST to form a large-scale partnership inclusive of the private sector, public sector and academia focusing on transition to post quantum cryptography based on the NIST Cryptographic Standards and Guidelines Development Process with the goal of speeding up the adoption and deployment of PQC. DHS and the Department of Commerce should encourage the adoption of post quantum cryptography in the public and private sectors by creating incentives to adopt PQC in federal systems and procurement, commercial ICT products, transport protocols, and underlying internet infrastructure.

Previous NSTAC reports, including the *NSTAC Report to the President on Communications Resiliency in 2021* and the *NSTAC Report to the President on a Cybersecurity Moonshot* in 2018, indicate that both adversaries and allies are advancing rapidly in quantum computing technologies and quantum resistant cryptography. Based on prior research and current member feedback on the urgent need to protect the U.S. from one of the most significant threats in the immediate future, the NSTAC recommends accelerating adoption of post quantum cryptography. This would require extensive industry participation and government and academia engagement.

4. Conclusion

Considering the broad use of ICT products in both critical and non-critical situations, it is time to ensure that security requirements are streamlined, evidence of compliance can be clearly identified, and users are given the necessary guidance to make informed choices about the products they use. This report advocates for structural changes to the way requirements are promulgated (with a strong effort to harmonize requirements to consensus standards), the way compliance with those requirements is demonstrated, and the way compliance is communicated to users.

It is critically important that sector experts be responsible for harmonizing enhanced (vertical) security requirements, and that there is a consistent way to collect and communicate compliance data so that users and regulators can more easily evaluate the security of ICT products.

In closing, three other points are worthy of note. First, the sheer number of ICT products and their almost infinite number of uses can cause decisional paralysis when it comes to compliance. Every potential model can be criticized, but the enemy of the good is the perfect. It is time to make some fundamental changes, learn from experience, and continue to innovate and iterate as products, services, software development models, operational practices, user behavior, and threat models all continue to evolve. This includes, in part, focusing on security outcomes and not specific implementations that cannot be adjusted as circumstances warrant.

Second, it is important that security assurance be the subject of consensus standards and international negotiations among industry and governments. ICT products are used globally and creating unnecessary "regulatory borders" can increase complexity and add costs without improving security. If there are genuine security issues that are unique to a jurisdiction, then enhanced security requirements should be added on top of commonly agreed-upon security baselines. But, otherwise, leveraging existing best practices and consensus standards and aligning requirements and conformance verification methods to the greatest extent practicable across sectors and across the globe allows for efficient reuse of certifications and related artifacts or evidence.

Finally, there must be a continued focus on automation. One of the great challenges in improving computer security relates to scale. For example, many have advocated for better computer security education for developers and operators. Of course, education is a good thing and should be encouraged, but the sheer number of developers and operators – including very small entities with extremely tight budgets and little bandwidth for training – means the country cannot educate its way out of the computer security problem. Instead, it must focus on automating all aspects of computer security. Improving cybersecurity will require tools that can automate communicating requirements, securing development and operations, producing artifacts of conformance, and communicating that conformance to others. Simply put, only with automation can security be scaled.

Appendix A. Earlier Study Phases Summaries

A.1. Phase I: Software Assurance in the Information and Communications Technology (ICT) and Services Supply Chain

The President's National Security Telecommunications Advisory Committee's (NSTAC) Phase I report focuses on software assurance and the ICT and services supply chain. The issue is important because of software supply chain compromises that highlighted critical risks and the large-scale ramifications for industry and government. The study delivers a broad range of findings primarily based on increasing security during the software development process and improving software supply chain risk management practices. The findings and recommendations are categorized into three areas: software assurance, stakeholders, and the external factors affecting software assurance.

A.1.1. Software Assurance

The findings state that there is not one software assurance approach that works in all situations, that open source software is not intrinsically less secure but requires different security incentives, that different stakeholders (developers, maintainers, procurement workers) have differing objectives that are sometimes in tension, that provable evidence of assurance is difficult to obtain based on current practices and that best practices in software assurance are not being developed fast enough. The report also observes that there are no viable globally applicable incentives for software assurance and that higher education has not developed curriculum for an organic approach to software assurance, which necessitates the need for on-the-job training for university graduates.

The opening recommendation advises that "**the president should establish a task force charged with defining a private-public initiative focusing on key areas of software assurance and the software supply chain. Like the earlier public-private effort on the [National Institute of Science and Technology] NIST Cybersecurity Framework (CSF),[67] such an initiative can address fundamental misalignment of incentives, diversity of the assurance approaches, and complexity of the software supply chain.**"[68]

Further recommendations focus on adoption of supply chain risk management practices adapted to the modern software ecosystem, using public-private efforts to improve security assurance standards, government investment in research and development (R&D) for the software assurance field to keep up with advances in computing architectures, and improving security and assurance processes for open source software. The following paragraphs include key points for each of these areas and related developments that occurred after the report was issued.

---

[67] "Framework Documents," NIST, accessed January 5, 2023, https://www.nist.gov/cyberframework/framework.

[68] President's NSTAC, "Report to the President on Software Assurance in the Information and Communications Technology and Services Supply Chain," November 2021, https://www.cisa.gov/sites/default/files/publications/NSTAC Report to the President on Software Assurance.pdf.

For adoption of supply chain risk management practices, key points for public-private sector collaboration are to identify, evaluate, and measure the effectiveness of new security assurance practices; develop and adapt standards to secure software build environments; reference the Department of Homeland Security's (DHS) ICT Supply Chain Risk Management (SCRM) Task Force[69] efforts as a baseline to assess threat mitigation relative to software assurance; and examine processes used by organizations focused on cybersecurity and software assurance, including industry sectors (e.g., telecommunications) to improve best practices, all while encouraging a diversity of developer organizations are adequately represented.

Key points for activities to improve harmonization among security assurance standards are to identify gaps, conflicting products, overlaps, and obsolescence in software security assurance standards, guidelines, and frameworks and to use the interagency process, public-private partnerships, and global leadership to support efforts such as the NIST CSF and the Secure Software Development Framework (SSDF).

To advance government investment in R&D for software assurance, Phase I includes these points: (1) support for government agencies and labs, academic research, and industry to address future computing architectures; (2) encouraging investment in innovation to automate software assurance tasks, including auditing, testing, collecting requirements, generating secure code, developing threat models, and software SCRM; and (3) strengthening emerging approaches in software assurance, such as using artificial intelligence (AI) and evidence-based data-driven metrics.

Since the Phase I report was issued, NIST published a draft SP 800-55 Rev. 2: Performance Measurement Guide for Information Security on November 14, 2022, for feedback.[70] Additionally, NIST published SP 800-218: SSDF Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities in February 2022, inclusive of guidance for protecting build environments and diverse industry feedback. Also in February 2022, NIST launched a Request for Information to improve the NIST CSF and Cybersecurity Supply Chain Risk Management as the start of a journey to develop version 2.0 of the NIST Cybersecurity Framework.[71]

A range of points are offered in Phase I to improve security and assurance processes for open source software. These include:

- Incentivizing collaboration between open source developers and organizations focusing on security, such as the Open Source Security Foundation (OpenSSF);[72]

---

[69] "Information and Communications Technology Supply Chain Risk Management Task Force," CISA, accessed January 5, 2023, https://www.cisa.gov/ict-scrm-task-force.

[70] Katherine Schroeder and Hung Trinh, "SP 800-55 Revision 2: Performance Measurement Guide for Information Security (initial working draft)," NIST, November 14, 2022, https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft.

[71] "Updating the NIST Cybersecurity Framework (CSF) – Journey To CSF 2.0," NIST, accessed January 5, 2023, https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

[72] "Open Source Security Foundation (OpenSSF)," The Linux Foundation Projects, accessed January 5, 2023, https://openssf.org/.

- Tasking NIST to extend efforts from its work related to EO 14028[73] to identify the top open source packages used for "critical software",

- Tasking the federal government to engage with organizations, allied nations, and government agencies outside of the U.S. (e.g., the European Union Agency for Cybersecurity (ENISA),[74] the G7, or the United Nations), to create and fund a public-private software assurance program to improve open source security;

- Developing standards to accurately describe software components, in collaboration with organizations such as OpenSSF and international standards bodies; and

- Encouraging developers to adopt a system of code vetting, such as OpenSSF's Scorecard 2.0.[75]

Subsequent to the publication of NSTAC's Phase I report, the White House held meetings focused on open source security, an example is the January 13, 2022, meeting that "convened government and private sector stakeholders to discuss initiatives to improve the security of open source software and ways new collaboration could rapidly drive improvements."[76] A short time later, on March 1, the OpenSSF announced the addition of 20 new members intending to help identify and fix security vulnerabilities in open source software and develop improved tooling, training, research, best practices and vulnerability disclosure practices. On May 12, 2022, the OpenSSF gathered industry and government leaders for an "Open Source Software Security Summit II" and announced pledges of over $30 million towards "10 streams of investments includ[ing] concrete action steps for both more immediate improvements and building strong foundations for a more secure future."[77]

A.1.2. Stakeholders

Regarding stakeholders, the recommendations advise incentivizing collaboration and engagement among all stakeholders by enhancing standardization efforts; to encourage the creation of flexible assurance practices, via government procurement rules, documenting best practices, and promoting approaches used in NIST CSF and SSDF; and to reform government procurement and improve information sharing practices.

---

[73] The White House, "EO 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[74] "European Union Agency for Cybersecurity (ENISA)," ENISA, accessed January 5, 2023, https://www.enisa.europa.eu/.

[75] John Mertic, "Open Source Ecosystem Gains New Support for Securing the World's Most Critical and Pervasive Software," Open Source Security Foundation, The Linux Foundation Projects, July 28, 2021, https://openssf.org/press-release/2021/07/28/open-source-ecosystem-gains-new-support-for-securing-the-worlds-most-critical-and-pervasive-software/.

[76] The White House, "Readout of White House Meeting on Software Security," January 13, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/.

[77] OpenSSF, "The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II," May 12, 2022, https://openssf.org/press-release/2022/05/12/the-linux-foundation-and-open-source-software-security-foundation-openssf-gather-industry-and-government-leaders-for-open-source-software-security-summit-ii/.

A.1.3. External Factors

Recommendations focusing on external factors include the development of viable incentives via a private/public task force and harmonizing education and training requirements, and to improve university curriculum and foster changes in K-12 education.

A.2. Phase II: Zero Trust and Trusted Identity Management

NSTAC's Phase II report focuses on zero trust and trusted identity management. Zero trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur and, therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified. Zero trust is not a single technology, but many cybersecurity technologies can help enable the implementation of zero trust security principles.

Starting with the May 2021 Executive Order 14028 and the subsequent January 2022, Federal Zero Trust Strategy, the federal government has begun to take steps to advance federal agencies towards zero trust architectures. Published on the heels of the federal strategy's release, the February 2022 Phase II report provides strategic recommendations on how the U.S. government could most effectively implement the Federal Zero Trust Strategy and incentivize zero trust adoption across the broader national ecosystem. Towards this end, the report focuses on policy actions the U.S. government can take in the immediate term to institutionalize zero trust as a long-term cybersecurity strategy beyond the shorter-term 2.5 year focus of the Federal Zero Trust Strategy. The report identifies that a critical part of fostering that long-term commitment is providing assurance that zero trust initiatives are actually and measurably improving federal cybersecurity outcomes.

Security assurance is often best validated by widely agreed upon tools for measurement. As the report states, "Because zero trust is a process of continuous improvement, progress is best measured through the framework of a maturity model." The report also introduces several frameworks for measuring zero trust, including CISA's Zero Trust Maturity Model. The Zero Trust Maturity Model describes a continuum of zero trust implementation maturity for Agencies to measure against, from traditional, to advanced, to optimal. For example, an Agency with a traditional posture will have a simple, static snapshot inventory of all connected devices on their network. An Agency with an optimal posture can conduct continuous security monitoring of all devices and control user access to the device's data based on dynamic, real-time authentication.

Whether or not an Agency's security posture sits on the traditional or optimal end of the maturity spectrum is measurable and provable. Security tools currently exist that can produce artifacts that provide assurance that an Agency is complying with a defined security standard. For zero trust, the report recommends that "The Federal Chief Information Security Officer (CISO), working in close coordination with the National Cyber Director, should establish or enhance existing metric-based reporting requirements tied to industry best practices for zero trust implementation with reporting accountability at the Agency CISO-level or above." Agencies must thus demonstrate to the federal CISO that they are advancing zero trust architectures in line with the Federal Zero Trust Strategy through quantifiable reporting metrics.

A.3. Phase III: Information Technology and Operational Technology Convergence

NSTAC's Phase III report on the convergence of information technology (IT) and operational technology (OT) focuses on the key challenges of securing OT systems against threats that emerge from connecting OT and IT networks and includes recommendations to identify emerging approaches to increase OT resiliency, including adaptations of IT security approaches to address OT security challenges.

Many organizations have connected IT and OT systems to leverage data that is generated to drive greater efficiencies and provide better services. However, this interconnectivity has exposed OT systems, many of which have been in service for decades, to cyber threats against which they were not designed to defend. The NSTAC was tasked with developing recommendations to improve the security of converged IT and OT systems.

The NSTAC found that IT/OT convergence has been happening for decades and that the United States has the technology and knowledge to secure these systems. However, the country has not prioritized the resources required to implement these solutions. In addition, many organizations lack visibility into their complete OT environments, including IT/OT interconnections and supply chain dependencies. Further, stakeholders too often choose to "bolt on" security in OT environments after the fact, rather than proactively "build in" security in the design and development of these systems. Public and private sector procurement vehicles and requests for proposals for OT systems and technologies rarely require or adequately value cybersecurity capabilities. And, while government regulations may be necessary to help improve infrastructure security in certain instances, these regulations should be flexible, outcomes-oriented, consensus standards-based, and vendor agnostic, and they should promote interoperability.

To address these challenges, the NSTAC Phase III report outlines 15 recommendations to help improve the security of converged IT/OT systems in both the public and private sectors. Among these recommendations, the NSTAC identifies three recommendations for the president to implement, which would provide immediate improvement for the cybersecurity posture of United States government-owned and operated OT systems, and which could serve as a model for private sector OT cybersecurity best practices.

First, the NSTAC report recommends that CISA issue a binding operational directive (BOD) to require federal civilian branch Agencies to maintain a real-time, continuous inventory of all OT devices, software systems and assets, including an understanding of any interconnectivity to other systems. NSTAC found that public and private sector organizations have limited visibility into what IT and OT assets they own and operate, and into how these systems and devices are interconnected with enterprise or other networks. Requiring federal Agencies to inventory these assets will increase organizational visibility and help cybersecurity teams prioritize plans, budgets, and resources in a risk-informed manner. In addition to or as an alternative to having CISA issue a BOD, the administration can task NIST with updating Federal Information Security Management Act (FISMA) guidance to achieve the same objective. These requirements should be made publicly available for state, local, tribal, and territorial (SLTT) government and private sector entities to adopt these practices.

Following NSTAC's Phase III report, CISA issued BOD 23-01[78] on October 3, 2022, that directed federal civilian Agencies to perform automated weekly asset discovery and vulnerability enumeration of all IP-addressable networked assets, including both IT and OT assets. The BOD is consistent with the NSTAC recommendation outlined above.

Second, the Phase III report recommends that CISA develop guidance on updating and enhancing IT/OT products and services procurement language to incentivize the inclusion of risk-informed cybersecurity capabilities within delivered products and services. This guidance, which can be developed in partnership with NIST, should be incorporated by the General Services Administration into federal government procurement vehicles to ensure that cybersecurity is adequately weighed in the acquisition of IT and OT products and services. This guidance should also be developed and published in a manner to make it easily adoptable by SLTT government and private sector owners and operators of OT systems for their own procurement vehicles and requests for proposals.

Third, the NSTAC report recommends that the National Security Council, CISA, and the Office of the National Cyber Director (ONCD) prioritize the development of interoperable, technology-neutral, vendor-agnostic, information-sharing mechanisms to enable real-time sharing of collective defense information amongst authorized critical infrastructure stakeholders. Similar cyber-attacks often target multiple industry sectors and government agencies. Information silos within and across agencies inhibit effective cybersecurity protection, detection, and response. Developing and implementing open, standards-based information sharing mechanisms will enable the broader ecosystem to pool cyber intelligence, identify potential threats and attacks, and disseminate mitigation strategies in an expedited manner, significantly reducing the risk of systemic, cross-sector attacks.

As assurance may require a combination of regulations, standards, certification and guidance, the Phase III report also recommends that ONCD, in collaboration with CISA, initiate an interagency study to assess conflicting regulations for OT operators that apply to the same sector. Based on the results of this study, the ONCD and CISA should recommend opportunities to synchronize conflicting requirements, which can simplify the regulatory landscape.

[78] CISA, "Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks," October 3, 2022, https://www.cisa.gov/binding-operational-directive-23-01.

Appendix B. Membership and Participants

Table 1: Subcommittee Leadership

Name	Organization	Role
Mr. Scott Charney	Microsoft Corp.	Subcommittee Chair
Mr. Kevin Reifsteck	Microsoft Corp.	Working Group Co-Lead
Mr. Robert Spiger	Microsoft Corp.	Working Group Co-Lead

Table 2: Subcommittee Membership

Name	Organization
Mr. Christopher Anderson	Lumen Technologies, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. Jamieson Brown	Tenable Holdings, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Victor Einfeldt	Iridium Communications, Inc.
Ms. Katherine Gronberg	NightDragon Management Company
Mr. Kent Landfield	Trellix
Dr. Nandi Leslie	Raytheon Intelligence and Space
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Richard Mosley	AT&T, Inc.
Dr. Anne Murray	Raytheon Intelligence and Space
Dr. Elaine Newton	Oracle Corp.
Mr. Thomas Quillin	Intel Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Dr. Claire Vishik	Intel Corp.

Table 3: Briefers, Subject-Matter Experts

Name	Organization
Mr. Daniel Bardenstein	Cybersecurity and Infrastructure Security Agency (CISA)
Mr. Brad Behm	Amazon Web Services, Inc.
Mr. Michael Bergman	Consumer Technology Association
Mr. Henk Birkholz	Fraunhofer Institute for Secure Information Technology
Mr. John Boyens	National Institute of Standards and Technology (NIST)
Mr. Mark Bunn	CISA
Ms. Lisa Carnahan	NIST
Mr. Rocky Campione	Amazon Web Services, Inc.
Mr. Wilson Co	Department of Treasury (DOT)
Mr. Christopher DeRusha	Office of Management and Budget (OMB), Office of the National Cyber Director
Mr. Martin Edwards	Tenable Holdings, Inc.
Mr. Cédric Fournet	Microsoft Corp.
Mr. Gordon Gillerman	NIST
Ms. Barbara Guttman	NIST
Ms. Debra Jordan	Federal Communications Commission (FCC)
Ms. Lauren Kravetz	FCC
Mr. Robert Martin	MITRE
Mr. Milad Maleki	United States Department of the Treasury (DOT)
Mr. Matthew McCabe	Kivu Consulting
Ms. Katerina Megas	NIST
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Richard Mosley	AT&T, Inc.
Mr. Rohan Paris	DOT

Name	Organization
Mr. Brian Peretti	DOT
Mr. Thomas Quillin	Intel Corp.
Mr. Adam Sedgewick	NIST
Mr. Orie Steele	Transmute Industries
Ms. Angela Smith	NIST
Mr. Thomas Smith	General Services Administration (GSA)
Mr. Murugiah Souppaya	NIST
Ms. Rosa Underwood	GSA
Dr. Claire Vishik	Intel Corp.
Mr. Mitchell Wander	DOT
Ms. Rita Young	OMB

Table 4: Subcommittee Management

Name	Organization
Ms. DeShelle Cleghorn	President's National Security Telecommunications Advisory Committee (NSTAC) Alternate Designated Federal Officer (ADFO)
Mr. Scott Zigler	NSTAC ADFO
Ms. Laura Penn	Edgesource Corp.
Mr. Joel Vaughn	TekSynap Corp.

Appendix C. Acronyms

Table 5: Acronyms

Acronym	Definition
AI	Artificial Intelligence
BOD	Binding Operational Directive
CDM	Continuous Diagnostics and Mitigation
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cross-Sector Performance Goal
CQSMO	Cybersecurity Quality Service Management Office
DHS	Department of Homeland Security
ENISA	European Union Agency for Cybersecurity
EO	Executive Order
FISMA	Federal Information Security Management Act
GSA	General Services Administration
ICS	Industrial Control Systems
ICT	Information Communication Technology
ISO/IEC	International Organization for Standardization/International Electrotechnical
IT	Information Technology
NIST	National Institute of Standards and Technology
NSM	National Security Memorandum
NSTAC	President's National Security Telecommunications Advisory Committee
OCRH	Office of Cybersecurity Regulatory Harmonization
OIRA	Office of Information and Regulatory Affairs

Acronym	Definition
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OPM	Office of Personnel Management
OT	Operational Technology
PLC	Programmable Logic Controllers
R&D	Research and Development
SBOM	Software Bill of Material
SCITT	Supply Chain Integrity, Transparency and Trust
SLTT	State, Local, Tribal, and Territorial
SP	Special Publication
SRMA	Sector Risk Management Agency
SSDF	Secure Software Development Framework
U.S.	United States
U.S.C.	United States Code
USG	United States Government

Appendix D. Definitions

Table 6: Definitions

Term	Definition	Source
Artificial Intelligence	(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. (2) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.	▪ American National Standards Institute International Committee for Information Technology Standards 172-220 (R2007) Information Technology -- American National Standard Dictionary of Information Technology ▪ Cited in NIST's *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*
Connectivity	Capacity for interconnecting platforms, systems, and applications.	▪ PCMag, https://www.pcmag.com/encyclopedia/term/connectivity
Critical Infrastructure	Sixteen sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.	▪ Cybersecurity Infrastructure Security Agency, https://www.cisa.gov/critical-infrastructure-sectors
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.	▪ NIST, https://csrc.nist.gov/glossary/term/cryptography

Term	Definition	Source
EO 14028, Improving the Nation's Cybersecurity	Charges multiple agencies, including NIST, with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.	▪ Federal Register: Improving the Nation's Cybersecurity
Hardware	The physical components of an information system.	▪ NIST SP 800-53 Rev. 4 under Hardware CNSSI 4009
Industrial Control System (ICS)	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy)	▪ NIST, https://csrc.nist.gov/glossary/term/industrial_control_system

Term	Definition	Source
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.	▪ Federal Information Processing Standards 200 under Information Technology 40 U.S.C., Sec. 1401
Malware	Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.	▪ CNSSI 4009-2015 under malicious logic from Internet Engineering Task Force Request for Comments 4949 V2
National Security and Emergency Preparedness	Policies, plans, procedures, and readiness measures that enhance the ability of the U.S. government to mobilize for, respond to, and recover from a national security emergency.	▪ Department of the Interior, https://www.doi.gov/sites/doi.gov/files/-900-dm-5-nsep-2021.pdf

Term	Definition	Source
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.	▪ NIST SP 800-37 Rev. 2
Protocol	A set of rules governing the exchange or transmission of data between devices.	▪ Britannica, https://www.britannica.com/technology/protocol-computer-science
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS.	▪ NIST SP 800- 53, CNSSI 4009, Adapted
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).	▪ NIST SP 800-161 under Verification from CNSSI 4009 (Revised May 2022: https://doi.org/10.6028/NIST.SP.800-161r1) ▪ ISO 9000 – Adapted ▪ NISTIR 7622 under Verification from CNSSI 4009, ISO 9000 – Adapted

Term	Definition	Source
Zero Trust	A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.	▪ NIST SP 800-207, https://doi.org/10.6028/NIST.SP.800-207
Zero Trust Architecture	An architecture that treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized.	▪ NIST, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

Appendix E. Bibliography

Amazon Web Services (AWS). "AWS Compliance Programs." Accessed January 4, 2023. https://aws.amazon.com/compliance/programs/.

Bardenstein, Daniel, Cybersecurity and Infrastructure Security Agency (CISA). "CISA's Cybersecurity Performance Goals." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Strategy for Increasing Trust Subcommittee, Arlington, VA, September 20, 2022.

Behm, Bradley, Amazon Web Services, Inc. "Strategy for Increasing Trust Subcommittee Briefing." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Strategy for Increasing Trust Subcommittee. Arlington, VA, September 8, 2022.

Bergman, Mike, Consumer Technology Association. "A Private Sector Assurance Program for Minimum Security Standards-The National Cybersecurity Label Project." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, August 18, 2022.

Birkholz, Henk, Fraunhofer Institute for Secure Information Technology, and Fournet, Cédric, Microsoft, and Martin, Robert, MITRE, and Steele, Orie, Transmute Industries. "Supply Chain Integrity, Transparency and Trust." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, September 15, 2022.

Boyens, Jon et al. "SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." National Institute of Standards and Technology (NIST), May 2022. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final.

Boyens, Jon, and Guttman, Barbara, and Megas, Katerina, and Smith, Angela, and Souppaya, Murugiah, NIST, Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, November 1, 2022.

Bunn, Mark, CISA. "Considering Security in Information Technology and Operational Technology Procurement." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, November 17, 2022.

Campione, Rocky, Amazon Web Services. "Experiences from the field: Building Future Compliance to Promote Security and Innovation." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, October 6, 2022.

Carnahan, Lisa, and Gillerman, Gordon, and Sedgewick, Adam, NIST. "Conformity Assessment: It Is About Confidence." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, October 13, 2022.

Co, Wilson, and Maleki, Milad, and Paris, Rohan, and Peretti, Brian, and Wander, Mitchell, U.S. Department of the Treasury. Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, October 25, 2022.

CISA. "Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks." October 3, 2022. https://www.cisa.gov/binding-operational-directive-23-01.

CISA. "Continuous Diagnostics and Mitigation." Accessed January 4, 2023. https://www.cisa.gov/cdm.

CISA. "Cross-Sector Cybersecurity Performance Goals." Accessed January 4, 2023. https://www.cisa.gov/cpg.

CISA. "Cross-Sector Cybersecurity Performance Goals." 2022. https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.

CISA. "Cyber Assessments." Accessed January 4, 2023. https://www.cisa.gov/cyber-assessments.

CISA. "Cyber Incident Reporting for Critical Infrastructure Act of 2022." Accessed January 5, 2023. https://www.cisa.gov/circia.

CISA. "Cyber Incident Response." Accessed January 4, 2023. https://www.cisa.gov/cyber-incident-response.

CISA. "Cybersecurity Training and Exercises." Accessed January 4, 2023. https://www.cisa.gov/ cybersecurity-training-exercises.

CISA. "Cybersecurity Quality Services Management Office (Cyber QSMO)." Accessed January 4, 2023. https://www.cisa.gov/cyber-qsmo.

CISA. "High-Value Asset Program Management Office." Accessed January 4, 2023. https://www.cisa.gov /hva-pmo.

CISA. "Information and Communications Technology Supply Chain Risk Management Task Force." Accessed January 5, 2023. https://www.cisa.gov/ict-scrm-task-force.

CISA. "National Cybersecurity Protection System." Accessed January 4, 2023. https://www.cisa.gov/ national-cybersecurity-protection-system-ncps.

CISA. "Trusted Internet Connections." Accessed January 4, 2023. https://www.cisa.gov/tic.

CISA. "Zero Trust Maturity Model." Accessed January 5, 2023. https://www.cisa.gov/zero-trust-maturity-model.

DeRusha, Chris, Office of Management and Budget (OMB). Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, December 8, 2022.

Edwards, Marty, Tenable Holdings, Inc. "Increasing Trust in the Information and Communications Technology and Services Ecosystem." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, August 30, 2022.

European Union Agency for Cybersecurity (ENISA). "ENISA." Accessed January 5, 2023. https://www.enisa.europa.eu/.

Federal Communications Commission (FCC). "Chairwoman Rosenworcel to Lead Federal Interagency Cybersecurity Forum." February 3, 2022. https://www.fcc.gov/document/chairwoman-rosenworcel-lead-federal-interagency-cybersecurity-forum.

Google Cloud. "Compliance Offerings." Accessed January 5, 2023. https://cloud.google.com/security/compliance/offerings.

Internet Engineering Task Force (IETF). "Supply Chain Integrity, Transparency, and Trust: An open collaboration space to incubate Internet-Drafts for the IETF focusing on a global initiative for securing end-to-end supply chains." GitHub (Internet hosting service), accessed January 5, 2023. https://github.com/ietf-scitt?msclkid=020292bba6db11ec8569eadc629a068c.

Johnson, Lamar. "FCC Interagency Cybersecurity Forum to Focus on Harmonizing Private-Public Cyber." Meritalk, April 11, 2022. https://www.meritalk.com/articles/fcc-interagency-cybersecurity-forum-to-focus-on-harmonizing-private-public-cyber/.

Jordan, Debra, and Kravetz, Lauren, FCC. "Harmonizing Cybersecurity Regulations Across Sectors." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, November 15, 2022.

McCabe, Matthew, Kivu Consulting. Briefing to the NSTAC Strategy for Increasing Trust Subcommittee. Arlington, VA, August 30, 2022.

Mertic, John. "Open Source Ecosystem Gains New Support for Securing the World's Most Critical and Pervasive Software." Open Source Security Foundation (OpenSSF), The Linux Foundation Projects, July 28, 2021. https://openssf.org/press-release/2021/07/28/open-source-ecosystem-gains-new-support-for-securing-the-worlds-most-critical-and-pervasive-software/.

Microsoft. "Azure Compliance Documentation." Accessed January 5, 2023. https://learn.microsoft.com/en-us/azure/compliance/.

Microsoft. "HAFNIUM Targeting Exchange Servers with 0-day Exploits." March 2, 2021. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers.

Microsoft. "Microsoft Digital Defense Report 2022." 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

MITRE ATT&CK." SUNSPOT." January 12, 2021. https://attack.mitre.org/software/S0562/.

Morgan, Sean, Palo Alto Networks, Inc. "Overview-Enhancing Internet Resilience Phase II Subcommittee on Zero Trust and Trusted Identity Management." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, August 23, 2022.

Mosely, Richard, AT&T, Inc. "NSTAC Letter to the President on Findings and Recommendations for Technology Standards." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, August 25, 2022.

National Institute of Standards and Technology (NIST). "Attestation." Accessed January 4, 2023. https://csrc.nist.gov/glossary/term/attestation.

NIST. "Automated Cryptographic Validation Testing." NIST.gov, Accessed January 4, 2023. https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing.

NIST. "Framework Documents." Accessed January 5, 2023. https://www.nist.gov/cyberframework/framework.

NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." April 26, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NIST. "Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order." Accessed January 4, 2023. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity.

NIST. "NIST Interagency Report 7977 - Cryptographic Standards and Guidelines Development Process." March 2016. https://csrc.nist.gov/publications/detail/nistir/7977/final.

NIST. "Security Assurance." Accessed January 4, 2023. https://csrc.nist.gov/glossary/term/ security_assurance.

NIST, "SP 800-53B: Control Baselines for Information Systems and Organizations." October 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

NIST, "SP 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations." September 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

NIST. "Updating the NIST Cybersecurity Framework (CSF) – Journey To CSF 2.0." Accessed January 5, 2023. https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

Office of Information and Regulatory Affairs (OIRA), OMB, Executive Office of the President (EOP). "Frequently Asked Questions." Accessed January 5, 2023. https://www.reginfo.gov/public/jsp/Utilities/faq.jsp#reg_rule.

OMB, EOP, "M-21-30: Protecting Critical Software Through Enhanced Security Measures." August 10, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf.

OMB, EOP, "M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

OMB, EOP, "M-21-30: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices." September 14, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

OpenSSF. "The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II." May 12, 2022. https://openssf.org/press-release/2022/05/12/the-linux-foundation-and-open-source-software-security-foundation-openssf-gather-industry-and-government-leaders-for-open-source-software-security-summit-ii/.

Oracle. "Oracle Cloud Compliance." Accessed January 4, 2023, https://aws.amazon.com/compliance/programs/.

President's NSTAC. "NSTAC Report to the President on Software Assurance in the Information and Communications Technology and Services Supply Chain." November 2021. https://www.cisa.gov/sites/default/files/publications/NSTAC Report to the President on Software Assurance.pdf.

President's NSTAC. "NSTAC Report to the President on Information Technology and Operational Technology Convergence." August 2022. https://www.cisa.gov/nstac-publications.

President's NSTAC. "NSTAC Report to the President on Zero Trust and Trusted Identity Management." February 2022. https://www.cisa.gov/nstac-publications.

Quillin, Thomas, and Vishik, Claire, Intel Corp. "Summary of Findings and Next Steps: NSTAC Software Assurance Study." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, August 30, 2022.

Reginfo.gov. "Executive Order 12866 of September 30, 1993: Regulatory Planning and Review." October 4, 1993. https://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf.

Smith, Brad. "Defending Ukraine: Early Lessons from the Cyber War." Microsoft (blog), June 22, 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Smith, Tom, and Underwood, Rosa, General Services Administration. "A More Resilient Digital America." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, November 10, 2022.

Souppaya, Murugiah, Scarfone, Karen, and Dodson, Donna. "SP 800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities." NIST, February 2022. https://csrc.nist.gov/publications/detail/sp/800-218/final.

Transportation Security Administration. "Security Directives and Emergency Amendments." Accessed January 4, 2023. https://www.tsa.gov/sd-and-ea.

The Linux Foundation Projects. "OpenSSF." Accessed January 5, 2023. https://openssf.org/.

The White House. "Circular No. A-130: Managing Information as a Strategic Resource." 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

The White House. "Executive Order (EO) 14028: Improving the Nation's Cybersecurity." May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

The White House. "FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity." October 11, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/.

The White House. "Office of the National Cyber Director." Accessed January 5, 2023. https://www.whitehouse.gov/oncd/.

The White House. **"**Readout of White House Meeting on Software Security." January 13, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/.

U.S. Congress. "Consolidated Appropriations Act, 2022." March 15, 2022. https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

U.S. Congress. "Fiscal Year 2021 National Defense Authorization Act." November 12, 2021. https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf.

U.S. House of Representatives. "44 USC 3502: Definitions." Accessed January 5, 2023. https://uscode.house.gov/view.xhtml?req=(title:44%20section:3502%20edition:prelim).

Young, Rita, OMB. "OIRA 101: OIRA's Role in Harmonizing Regulations and Maximizing Net Benefits to Society." Briefing to the NSTAC Strategy for Increasing Trust Subcommittee, Arlington, VA, October 27, 2022.