The U.S. National Cybersecurity Strategy: A Vehicle with an International Journey

Jami M. Carroll
Harvard University, Somerset, MA, USA

jcarroll@prisidian.com

Abstract: The *U.S. National Cybersecurity Strategy* is focused on the five pillars of defending critical infrastructure: detect, disrupt, and dismantle threat actors; improve market resilience and security; invest in future resilience; and create international partnerships with shared goals. The National Cybersecurity Strategy Implementation Plan is focused on critical infrastructure supporting energy, financial, healthcare, information technology, and manufacturing sectors. In the U.S. alone, the SolarWinds supply chain attack affected nine federal agencies and about 100 companies. Ransomware attacks such as the Colonial Pipelines, the largest U.S. oil pipeline, disrupted supplies of gasoline and fuel to the U.S. East Coast and the JBS USA as the largest meat processor ransomware attack affecting one-fifth of the nation's meat supply. The *U.S. National Cybersecurity Strategy* as a response to the U.S.'s critical infrastructure concerns led to the creation of two core cybersecurity documents which were crafted jointly with several other allies. Cybersecurity and Infrastructure Security Agency (CISA) crafted the *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software* with joint agreement with National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and 15 international government agencies to give international vendors a roadmap of the expected cybersecurity hygiene required from their products. (CISA, 2023a; Car & De Luca, 2022) Building on the *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*, CISA, FBI and NSA met with cybersecurity organizations from Australia, Canada, New Zealand, and United Kingdom and jointly created *The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously* as a core issue identified in the earlier guidance. (CISA, 2023c). These two jointly led by the U.S. helped initiate an international cybersecurity norm insisting international software manufacturers demonstrate product security and transparency in the products they sell. These joint documents quickly showed how a global community can rally to solve cybersecurity challenges that have existed for decades. This led to twenty of the largest international software vendors creating the Minimum Viable Secure Product (MSVP) Working Group to address the requirements levied by these documents; CISA has joined this working group to help shape procurement, contractual controls, self-assessment, and system development lifecycle (SDLC) with these vendors. (CISA, 2024d; MSVP, n.d.) This research argues that the U.S. National Security Council (NSC) should leverage the talent pool of CISA, National Institute of Standards and Technology (NIST), Department of Defense (DoD), FBI, and NSA to improve detection, information sharing, security standards, and implementation for not only the U.S.'s government and commercial sectors, but also helps our allies and partners. The DoD and Office of the Director of National Intelligence (ODNI) have made great strides in improving security by integrating improvements with Zero Trust Architecture (ZTA), Supply Chain Risk Management (SCRM), Software Supply Chain Security, Cybersecurity Safety Review Board (CSRB), Cybersecurity Incident & Vulnerability Response Playbooks, and DoD National Security Systems (NSS) standards. The NSC should coordinate through CISA to develop a collaborative effort to not only benefit the U.S. critical infrastructure but also help our allies and partners.

Keywords: National Cybersecurity Strategy, critical infrastructure attacks, zero trust architecture, supply chain risk management, software supply chain security

1. Introduction

Disclaimer: All statements of fact, opinion, or analysis expressed are those of the author. The views and opinions expressed herein by the author do not represent the official policies or positions of the United States (U.S.) Department of Defense (DoD), U.S. Navy, or other agencies or departments of the U.S. government and are solely representative of the views of the author. This does not constitute an official release of DoD or Navy information.

The research methodology used in this research will be a survey methodology based on U.S. cybersecurity practices that shape international norms and could be collaborated on with allies. This research methodology starts with unfolding the Biden-Harris *U.S. National Security Strategy*. A literature review of the documents that evolved from this strategy will cover the two jointly created documents with allies, and the frameworks of ZTA, SCRM, Software Supply Chain Security, Cybersecurity Safety Review Board (CSRB), Cybersecurity Incident & Vulnerability Response Playbooks that allies could leverage and expand international cybersecurity norms with the U.S.

The Biden-Harris *U.S. National Security Strategy* is a cornerstone to protecting, improving, and maintaining the security of U.S. vital national interests, especially those things deemed critical infrastructure. It helps ensure economic prosperity and opportunity for the U.S. while laying out a plan that protects our critical infrastructure as it supports our democratic values and way of life. Most nations have similar interests that are highly compatible with ours and "we will build the strongest and broadest possible coalition of nations that seek to

cooperate with each other, while competing with those powers that offer a darker vision and thwarting their efforts to threaten our interests." (Biden, 2022, 7) Supply chain resiliency regardless of the product whether manufacturing, mining, Defense Industrial Base (DIB), or critical infrastructure is key to a nation's national security.

In 1998, President Clinton released PDD-63, *Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection: Sector Coordinators* where he defined critical infrastructures are those essential systems with a cyber-based and physical capability critical to the "minimum operations of the economy and government" with banking, energy, emergency services, finance, telecommunications, transportation, and water whether they are owned by the government or the commercial entities. (Clinton, 1998, 1) In 2000, Clinton released the *National Plan for Information Systems Protection* stating that cyber and the information revolution had touched every facet of our daily lives, whether the lights in our homes, boarding planes, or contacting loved ones since they all used critical infrastructure. Even our sophisticated Department of Defense (DoD) systems rely on computer-controlled capabilities and networks which could affected by intrusion and destruction if they become vulnerable. These commercial and defense segments could have catastrophic impacts on our economic sectors and government agencies if we fall prey to its peril. New approaches to the evolution of computers and their threats are tantamount to understanding the threats to critical infrastructure. We must create measures to safeguard these capabilities to gain all the benefits of the Information Age. (Clinton, 2000) In July 2000, The Commission on America's National Interests designated the U.S. critical infrastructure as "vital" and that the "U.S. critical infrastructure be reasonably resistant to concerted, sophisticated cyber-attack." (Allison & Blackwill, 2000, p. 48-49.) The U.S. Cybersecurity & Infrastructure Security Agency (CISA) was created in 2018 as a component under the U.S. Department of Homeland Security focusing on cybersecurity and critical infrastructure across the U.S. working with government agencies and the private sector; they work in collaboration with government and private sectors focusing on the U.S. critical infrastructure sectors listed in Table 1. (CISA, n.d.)

CISA realized that many in the international community had similar goals of creating a more resilient cybersecurity posture for their critical infrastructure like what was evolving from the U.S.'s *U.S. National Security Strategy* but crafted jointly for an international community. CISA requested comments of these joint goals in the *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*. This CISA released, joint document captured the goals of Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), Cyber Security Agency of Singapore (CSA), Computer Emergency Response Team New Zealand (CERT NZ), Cyber Security Centre New Zealand (NCSC-NZ), Czech Republic's National Cyber and Information Security Agency (NÚKIB), FBI, Germany's Federal Office for Information Security (BSI), Israel's National Cyber Directorate (INCD), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Korea Internet & Security Agency (KISA), OAS/CICTE Network of Government Cyber Incident Response Teams (CSIRT) Americas, Netherlands' National Cyber Security Centre (NCSC-NL), Norway's National Cyber Security Center (NCSC-NO), NSA, and the United Kingdom's National Cyber Security Centre (NCSC-UK). (CISA, 2023a)

Table 1: U.S. Critical Infrastructure

U.S. Critical Infrastructure			
Chemical	Dams	Financial Services	Information Technology
Commercial facilities	Defense Industrial Base	Food and Agriculture	Nuclear Reactors, Materials, and Waste
Communications	Emergency Services	Government Facilities	Transportation Systems
Critical Manufacturing	Energy	Health Care and Public Health	Water and Wastewater

The U.S. Office if the National Cyber Director (ONCD) was created by Congress in 2021 as an advisor to the President as a component of the Executive Office of the President to spearhead the President's *National Cybersecurity Strategy* to coordinate a whole-of-government implementation of the strategy.

ONCD assisted President Biden with developing *U.S. President's Executive Order (EO) 14017, America's Supply Chain: A Year of Action and Progress* as a direct result of supply chain security concerns after the SolarWinds supply chain attack of 2020, Colonial Pipelines ransomware attack of 2021, and JBS USA ransomware attack of 2021. The SolarWinds attack affected nine federal agencies and about 100 U.S. companies; the Colonial Pipelines

ransomware attack disrupted supplies of gasoline and fuel to most of the U.S. East Coast; and the JBS USA ransomware attack affected the largest meat supply source in the U.S. and affected one-fifth of the nation's meat supply. Had good Cybersecurity Supply Chain Risk Management (C-SCRM) practices been in place, there is the likelihood that no impact or a significantly reduced impact would have occurred. EO 14017 focused on these 2020 and 2021 attacks while widening the focus to the six sectors of energy, transportation systems, food and agriculture, health care and public health, information technology and defense industrial base after assessments from the private sector, think tanks, academia, non-profits, non-government organization, and numerous government organizations. These focus areas were endorsed by the National Security Advisor, Jake Sullivan, and the Economic Policy / Director of the Economic Council, Brian Deese. EO 14017 directed our agencies to partner with our industrial bases to monitor, rebuild, and strengthen our supply chain management with added resilience. (Biden, 2021a)

EO 14028 expanded the improvements to the supply chain by also requiring Zero Trust Architecture (ZTA), improved federal/private sector threat intelligence sharing, modernizing federal government cybersecurity, enhancing C-SCRM, establishing a Cyber Safety Review Board (CSRB), improved detection, standardized response, investigation and remediation capabilities in response to cybersecurity vulnerabilities and incidents, and a renewed improvement with National Security Systems (NSS) security posture. In EO 14028, President Biden indicated that we must work with allies and partners to decrease vulnerabilities before they enter the global supply chain. This should entail improving international adoption of best practices with allies, partner nations, and even competitor nations so that industrial policies and global sourcing of products receive similar cybersecurity treatment in the source countries before they are shipped out to the U.S. and other nations. (Biden, 2021b).

2. Secure Your Supply Chains: A Recipe for Building the Best Products

NSA says it's critical to consider the ingredients of software, firmware, and hardware as the starting point to resilient C-SCRM. Over the past five years, cybersecurity software supply chains as one of the most critical elements that has affected the U.S.; some of the issues with cybersecurity software supply chains likely affect our allies and partners. (NSA, 2023a) Over the past five years, the NSA has seen cybersecurity software supply chains as one of the most critical elements in developing a solid Cybersecurity Supply Chain Risk Management (C-SCRM). Upon release of EO 14028, NSA, ODNI, and CISA led a collaborative partnership between the U.S. government and private organizations across multiple sectors which created the Enduring Software Framework (ESF) and a panel creating the *Securing the Software Supply Chain: Recommended Practices for Customers*. (NSA, 2022a; NSA, 2022b; NSA, 2022c) The NSA recommended process starts with the ingredients as the key and monitoring them through their lifetime:

- Analyze software planned to examine it before it is integrated so it can be managed,
- After deployment, identify vulnerabilities and develop mitigations to correct the vulnerabilities, and
- During operation, use incident management to detect and respond to vulnerabilities. (NSA, 2023a)

2.1 Software Security & Firmware

NSA argued that software security should focus on three key areas: using the Software Bill of Material (SBOM) to gain transparency into what software is used and what vulnerabilities it possesses; leveraging memory-safe programming languages to eliminate the largest percentage of vulnerabilities; and using ongoing vulnerability scanning, detection and mitigation to address problems as they arrive. Vulnerabilities related to SolarWinds and Log4j could have been mitigated early in the vulnerability mitigation process affecting hundreds of organizations had they used the SBOM. (NSA, 2022c)

The SBOM collects the provenance of the software from the standpoint of who created the software or if received from a software supplier, who provided the software whether open source or commercial software. EO 14028 mandates the SBOM for all U.S. federal agencies. This provenance of each piece of software gives an organization transparency in the software used or provided to others; supports risk identification, analysis, and management; and for U.S. federal customers to show their compliance with EO 14028. (Biden, 2021b).

The U.S. Office of Management and Budget (OMB) mandates the use of the SBOM for all federal agencies as directed by EO 14028 and directs federal agencies to refer to the National Institute of Standards and Technology (NIST) for secure software development practices. The SBOM can create an inventory, it includes a hash / digital signature representing the software package and includes a Vulnerability Exploitability eXchange (VEX) capability

that has a channel to report flaws and track vulnerabilities using key risk management tools like the National Vulnerability Database (NVD), OASIS Common Security Advisory Framework (CSAF), and several MITRE-developed tools and guidance like the MITRE Adversarial Tactics, Techniques, and Common Knowledge or (MITRE ATT&CK), MITRE Common Attack Pattern Enumeration and Classification (MITRE CAPEC). Using the VEX capability, suppliers and consumers can gain greater insight into what vulnerabilities exist with the software package. Apache CycloneDX is one of the most used SBOM tools. (CISA, 2022; NIST, 2022a; NIST, 2022b) Apache CycloneDX can provide numerous pieces of information that support cyber risk deduction; these CycloneDX capabilities include:

- Software Bill of Materials (SBOM)
- Software-as-a-Service Bill of Materials (SaaSBOM)
- Hardware Bill of Materials (HBOM)
- Machine Learning Bill of Materials (ML-BOM)
- Operations Bill of Materials (OBOM)
- Manufacturing Bill of Materials (MBOM)
- Bill of Vulnerabilities (BOV)
- Vulnerability Disclosure Report (VDR)
- Vulnerability Exploitability eXchange (VEX)
- Common Release Notes Format

Elements of these CycloneDX capabilities go into CycloneDX's object model attributes to display metadata, components, services, dependencies, compositions, vulnerabilities, formulation, and annotation; they are illustrated in Figure 1.

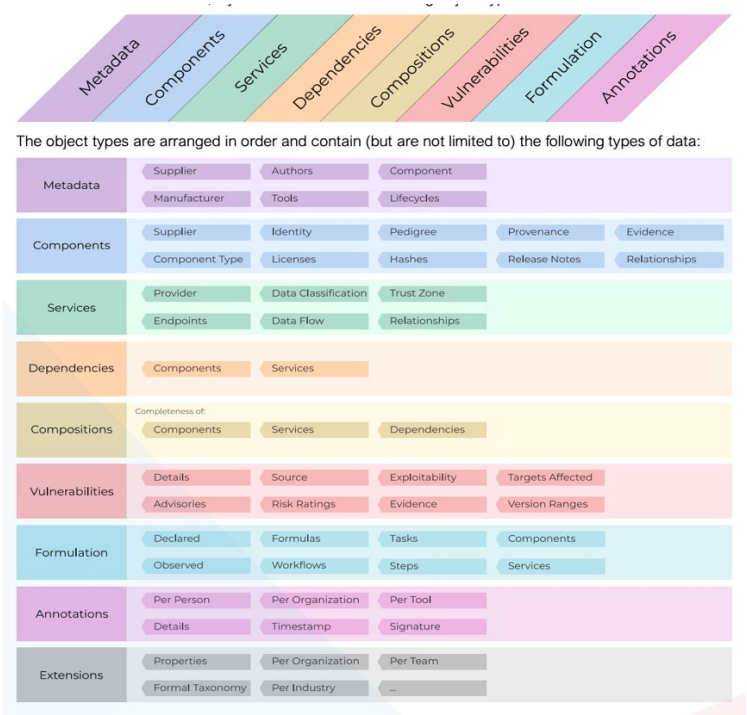

Figure 1: CycloneDX Object Model

NSA argued that 70% of most Common Vulnerability & Exposure (CVE) vulnerabilities have resulted because of memory-safe vulnerabilities. Using memory-safe programming languages (MSLs) like C#, Go, Java, Python, Rust, and Swift instead of C, C++, and Objective-C will correct most of these memory-safe vulnerabilities and enable a key process in the Secure by Design approach CISA and others laid out to eliminate most memory safety vulnerabilities. Security by Design leverages: 1) owning the security outcome, 2) developing radical transparency in development, and 3) employing a top-down security approach to ensure products developed are secure. To guide consumers wanting to leverage Security by Design, the U.S. CISA, FBI, and NSA collaborated with the Australian Signals Directorate's Australian Cyber Centre, Canadian Centre for Cyber Security, the United Kingdom's National Cyber Security Centre, New Zealand National Cyber Security Centre, and the Computer

Emergency Response Team New Zealand to develop *The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously*. (CISA, 2023c)

The last key area is vulnerability testing. Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) should be used throughout the development and test before becoming operational. SAST and DAST tools are commonly used in Development, Security, and Operations (DevSecOps) environments, but they can be used in non-DevSecOps environments. SAST tools look internally at the code as a static form of source, byte, or binary code to find code weaknesses. Many of these code weaknesses are from poorly created code such as using inappropriate coding practices or incorporating vulnerable libraries. SAST is extremely useful for looking at code in an early stage of development before it has been integrated with other capabilities. DAST looks at the code externally like it is a black box. DAST will look at runtime, environment, and logic that may make the code perform differently than expected. Quite often DAST tools will incorporate fuzzing to create situations where the code performs in an unexpected manner such as being able to order a negative 5 books or pay with a negative 10 dollars. (DoD, 2019; DoD, 2021) Once the system is built, before deployment and in operation, it should have ongoing vulnerability scanning, detection, and mitigation against the system. Vulnerability scanners are used to identify shortfalls in data encryption, opportunities for denial of service, privilege elevation, SQL injection, unauthorized access to data, and inappropriate user authentication and authorization. (NIST, 2022a).

Periodic vulnerability assessments and penetration testing are good forms of testing the system for potential vulnerabilities that may not have been captured by DAST and SAST or are recent vulnerabilities that have just recently developed. A vulnerability assessment is done to potentially find the possibility for exploitation without executing the exploitation. Penetration testing takes vulnerability assessment to the next step by exploiting the vulnerability. The process of vulnerability assessment and penetration testing follows a sequence of steps. That sequence is footprinting, fingerprinting, enumeration, research, escalation, repeat visits, and covering tracks using stealth so as not to become discovered, much like a hacker might execute their steps to stay hidden. The steps used in the vulnerability assessment inform the penetration tester of the possibility of threats, vulnerabilities, and impacts so that vulnerability analysis can be performed. This vulnerability analysis will focus on what vulnerabilities will have the biggest impact; the penetration test can use this analysis to perform the exploitation. Whether penetration testing is unannounced, only known to the leadership of the organization, or announced, known to the wider organization audience is determined by the rules of engagement set by the organization's leadership. Table 2 illustrates the general steps used in a vulnerability assessment and penetration testing effort. (Carroll, 2018)

Table 2: Typical Steps Used in Vulnerability and Penetration Testing of Systems

	Common Approaches	Description	Comments
Vulnerability Assessment	Footprinting	Where do the IP addresses/systems show up?	• Reconnaissance (active (scanning) or passive (sniffing) • External – DNS and external-facing systems (nslookup, whois, dig, SamSpade, NMAP, & Zone Transfer) • Internal – SNMP, Unix, Windows, LDAP, SMTP, & NMAP) *Note: Approach is slightly different if coming from inside the network than from outside the network*
Vulnerability Assessment	Fingerprinting	What are the ports and services for the OSs and Applications?	Fingerprinting (scanner with OS recognition)
Vulnerability Assessment	Enumeration	What version of a service exists? (Example – banner grabbing of a web server or mail server)	Enumeration, potential vulnerabilities
Vulnerability Assessment	Research	Common Vulnerability Database (CVE.mitre.org); National Vulnerability Database (http://nvd.nist.gov/);Open Source Vulnerability Database (www.osvdb.org)	
Penetration Test	Escalation	Privilege escalation, Denial of Service, Man in the Middle	Obtain access
Penetration Test	Repeat visits	Backdoors - Hackers do this - Pen Testers simulate unless authorized to perform destructive testing (DoD) - Computer Network Attack (CNA)/Computer Network Exploitation (CNE) may do this when authorized	Maintain Access
Penetration Test	Covering tracks	Log zappers, log stoppers - Hackers do this - Pen Testers simulate unless authorized to perform destructive testing (DoD) - Computer Network Attack (CNA)/Computer Network Exploitation (CNE) may do this when authorized	Erase evidence

2.2 Hardware / Firmware Security

NSA recommends that all enterprise servers, laptops, and desktops perform an automated acceptance test that includes secure boot (enabled), Trusted Platform Module (TPM) activated and enabled, and platform certificated that matches the components used in the system. This is usually done with a Unified Extensible Firmware Interface (UEFI)-enabled computer. Once all these features are initiated, they provide attestation that the computer has not been tampered with. Should the UEFI fail any tests, NSA recommends that the computer be considered defective and returned. (NSA, 2023b)

3. Zero Trust Architecture

Zero Trust Architecture (ZTA) moved away from having static perimeters that put all their trust in users, assets, and resources and move the trust based on the location or network the user is coming from and the resource they are trying to access. It treats all transactions as a workflow where trust is vetted before accessing assets, services, workflows, and network accounts. ZTA's security model is based on maintaining strict access controls and not trusting any entity by default, even those inside the network perimeter by ensuring micro-segmentation, continuous monitoring, and least privilege access of all assets with the architecture. ZTA calls also potentially reduce the effects of Distributed Denial of Service (DDoS) attacks. It does this by using network segmentation (NS), identity and access management (IAM), continuous monitoring and analytics (CMA), least privilege access (LPA), multi-factor authentication (LPA), and leveraging secure access service edge (SASE). (NIST, 2020) Table 3 rolls up the key features of the six major ZTA categories.

Table 3: Six Major ZTA Categories and their key features.

NS	IAM	CMA	LPA	MFA	SASE
Provides enhances security by using network segmentation to isolate critical resources, reduce attack surface, and improve overall security.	User authentication ensures users follow a strict mechanism or set of mechanism using MFA to gain access to resources.	Realtime threat detection ensures constant monitoring to help identify and respond to threats as they occur.	Minimal access granted to users that is specific to the permissions their specific role and tasks require – thus limiting damage from insider threat.	Enhances security by ensuring a layered defense with a combination of verification methods to validate the user's identity.	Cloud-Native Architectures can consolidate networking and security services in a cloud-delivered solution.
Controlled access to allow organization to monitor and control data moving between segments.	Extremely granular access control based on permissions and rights within the organization.	Anomaly recognition uses AI and Bayesian methods to detect unusual network behavior or unauthorized attempts to access organization resources.	Prevents over-privileging users with access to sensitive data, and thereby reducing the potential for data breaches or misuse.	User verification requires two or more verification factors, e.g. passwords, tokens, biometrics.	Edge protection ensures users and devices regardless of their location or network.
Reduced impact if a breach occurs as it will be limited to the single segment rather than the overall capability.	Continuous monitoring to track real-time user activities by the assigned credentials and mitigation of potential security risks.	Forensic analysis provides detailed investigation and post-incident analysis to improve the security posture of the capability for the future.			Integrates security through consistent policies and their enforcement across the organization.
Ensures compliance to meet regulatory and isolation of sensitive data within segments.					

4. Cybersecurity Safety Review Board

The Department of Homeland Security (DHS) created the Cybersecurity Safety Review Board (CSRB) because of President Biden's release of EO 14028. The CSRB looks at incidents where the worse of the worse threat actors, whether cybercrime syndicates or state actors have impacted major critical infrastructure, analyze their tactics, techniques, and procedures (TTP), the degree and type of impact so they can determine what additional security controls should be added. (CISA, 2023b; DHS, 2023) A CSRB is an independent entity comprised of highly qualified federal government and private sector members established to assess and analyze significant cybersecurity incidents that have impacted U.S. critical infrastructure. They conduct investigations into cyberattacks with the goal of understanding affected systems, vulnerabilities exploited, root causes of these exploits, and the impact they have had on the affected systems. The CSRB learns from past incidences and provides recommendations to prevent future occurrences to increase cybersecurity resilience. They seek to encourage cybersecurity transparency and accountability. Their comprehensive review often discovers evolving cyber threats and vulnerabilities previously not well known at the time, but through this review, they recommend the development

and implementation of more robust cybersecurity measures that can often be applied across multiple critical infrastructure sectors. The CSRB ultimately plays a critical role in maturing the U.S.'s critical infrastructure cybersecurity resilience through their detailed investigations which often provide significant insights into cyber incidents through their focus on transparency, accountability, and the potential for improved cybersecurity practices. (CISA, 2023b)

5. Cybersecurity Incident & Vulnerability Response Playbooks

The Cybersecurity Incident & Vulnerability Response Playbooks serve as a comprehensive guide so that organizations can effectively manage and respond to cybersecurity incidents. In the case of the U.S. federal government, there is whole-of-government roles and responsibilities citing several high-level government documents such as U.S. EOs, laws, and other mandatory requirements. One of the biggest benefits of the playbook is the standardized approach it provides to detecting, investigating, and mitigating cyber-related incidents in a play-by-play manner that walks the organization through the roadmap of events that should be accomplished during a cybersecurity crisis. The playbook structure covers best practices, guidelines, and procedures that the organization should do in a structured sequence. The emphasis on the early detection of cyber incidents is one of the greatest benefits. Other key benefits include recommended strategies to identify potential breaches at the earliest opportunity so that a swift response can be used resulting in minimal impact from the attackers thereby limiting the scope of the incident and giving the organization the greatest control over the incident. With the numerous steps that must be taken during an incident, the methodological approach leads the organization through a structured plan of action to understand the threat, vulnerability, impact, and mitigation steps. Along the way, this thorough investigation approach using the playbook helps to understand the threat landscape, vulnerabilities exploited, and the root cause of the breach; this provides critical threat intelligence about the incident that can be used to prevent similar attacks in the future. While every organization is different and has different vulnerabilities, threats, and impacts, the playbook is relatively tailorable to respond with the best response for that incident. There are sections on containment strategies, threat eradication, and mitigation approaches. Additionally, the playbook can serve as a training tool so that specific roles in organizations can enhance their response to upcoming incidents and ultimately improve their overall security posture. (CISA, 2021)

6. Conclusion

This paper argues that the proposed collaboration between the U.S. National Security Council (NSC) and key cybersecurity entities like CISA, NIST, DoD, NSA, and ONCD presents significant benefits for U.S. allies in terms of enhancing their cybersecurity capabilities which were jointly cosigned by several of the U.S.'s allies. CISA continues engaging international software vendors and collaborating with allies on cybersecurity norms. By leveraging this U.S. whole-of-government expertise and the resources they offer, allies and partners can significantly improve their detection, prosecution, and mitigation of cyber risks. Many of these advanced technologies and methods developed by these U.S. agencies could provide allies with cutting-edge tools to identify potential cyber threats more efficiently and accurately. These approaches could significantly improve the proactive stance of these allies against cyberattacks, reduce risks in their countries, and reduce risks affecting other countries. Information sharing is another critical area where U.S. allies could benefit – the collaboration outlined in this research could create a more open exchange of ideas related to cyber threat intelligence between the U.S. and its allies. Sharing of details from recent cyberattacks could better explain future, emerging threat vectors and provide indicators and warnings (I&W) allowing other nations to better prepare for attacks. A common collective defense approach could prepare other allies for the moving waves of attacks that go from region to region in their attacks. U.S. allies could benefit from the extensive set of security standards that NIST and other U.S. organizations have created. By adopting these standards, the overall global cybersecurity posture goes up amongst allied nations while knowing other adoptees have used similar approaches to protect their organizations. This mutual adoption could lead to common more effective cybersecurity across government organizations and private sectors which could bolster the globalization of trade, smoother cooperation, and greater interoperability with joint initiatives and operations. The integration of SCRM, ZTA, CSRB, and Cyber Incident Detection, Investigation, and Mitigation Playbook could serve as a blueprint for U.S. allies; although CISA and other U.S. agencies are leading these initiatives, strength in numbers could be achieved with more allies being involved. Learning from the U.S.'s approach to institutionalizing cybersecurity best practices, allies could help codify approaches leading to more resilient and responsive cybersecurity infrastructures, capable of withstanding and quickly recovering from cyberattacks. In essence, the collaborative effort spearheaded by the

CISA, NIST, DoD, NSA, and ONCD could offer a comprehensive model for strengthening global cybersecurity resilience, with U.S. allies standing to gain significantly from these initiatives.

References

Allison, G.T. and Blackwill, R., 2000. *America's National Interests: A Report From the Commission on America's National Interests*, The Commission on America's National Interests, July, https://www.belfercenter.org/sites/default/files/files/publication/amernatinter.pdf

Biden, J. R., 2021a. *The U.S. President's Executive Order (EO) 14017, America's Supply Chain: A Year of Action and Progress*, The White House, Washington, DC, https://www.whitehouse.gov/wp-content/uploads/2022/02/Capstone-Report-Biden.pdf

Biden, J. R., 2021b. *The U.S. President's Executive Order (EO) 14028, Improving the Nation's Cybersecurity*, The White House, Washington, DC, https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

Biden, J.R. (2022). *U.S. National Security Strategy*, The White House, Washington, DC, October, https://nssarchive.us/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Car, P. and De Luca, S., 2022. EU Cyber resilience act. *EPRS, European Parliament*, https://www.dimt.it/wp-content/uploads/2022/12/EPRS_BRI2022739259_EN.pdf

Carroll, J., 2018, June. Offensive and Defensive Cyberspace Operations Training: Are we There yet? In *European Conference on Cyber Warfare and Security* (pp. 77-86). Academic Conferences International Limited.

Clinton, W., 1998. *Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection: Sector Coordinators*. The White House, Washington, DC, May, https://www.govinfo.gov/content/pkg/FR-1998-08-05/pdf/98-20865.pdf

Clinton, W., 2000, *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0 An Invitation to a Dialogue*, The White House, Washington, DC, April, https://irp.fas.org/offdocs/pdd/CIP-plan.pdf

Cybersecurity & Infrastructure Security Agency (CISA), n.d., "Critical Infrastructure Sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

CISA, 2021, Cybersecurity Incident & Vulnerability Response Playbooks, [https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf]

CISA, 2022, Vulnerability Exploitability eXchange (VEX) – Use Cases, https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf

CISA, 2023a, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, https://www.govinfo.gov/content/pkg/FR-2023-12-20/pdf/2023-27948.pdf

CISA, 2023b, Review Of The Attacks Associated with Lapsus$ And Related Threat Groups Report, [https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf]

CISA, 2023c, *The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously,* https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf

CISA, 2024d, CISA Joins the Minimum Viable Secure Product Working Group, https://www.cisa.gov/news-events/news/cisa-joins-minimum-viable-secure-product-working-group

CycloneDX, n.d., Authoritative Guide to SBOM: Implement and Optimize Use of the Software Bill of Materials. https://cyclonedx.org/guides/sbom/OWASP_CycloneDX-SBOM-Guide-en.pdf

DHS, 2023, Cyber Safety Review Board Releases Report on Activities of Global Extortion-Focused Hacker Group Lapsus$, [https://www.dhs.gov/news/2023/08/10/cyber-safety-review-board-releases-report-activities-global-extortion-focused]

DoD, 2019, *DoD Enterprise DevSecOps Reference Design*, V 1.0, https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf

DoD, 2021, *DoD Enterprise DevSecOps Strategy Guide*, v 2.0, https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsStrategyGuide.pdf

MSVP, n.d., Minimum Viable Secure Product (MSVP), https://mvsp.dev/

NIST, 2020, NIST SP 800-207, Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

NIST, 2022a, *NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NIST, 2022b, *NIST SP 800-218, Secure Software Development Framework (SSDF) v1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

NSA, 2022a, NSA, CISA, ODNI Release Software Supply Chain Guidance for Developers. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3146465/nsa-cisa-odni-release-software-supply-chain-guidance-for-developers/

NSA, 2022b, ESF Partners, NSA and CISA Release Software Supply Chain Guidance for Customers, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3221208/esf-partners-nsa-and-cisa-release-software-supply-chain-guidance-for-customers/

NSA, 2022c, Securing the Software Supply Chain: Recommended Practices for Developers. https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF

NSA, 2023a, Recommendation for Software Bill of Materials (SBOM) Management, https://media.defense.gov/2023/Dec/14/2003359097/-1/-1/0/CSI-SCRM-SBOM-MANAGEMENT.PDF

NSA, 2023b, Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktops Computers, https://media.defense.gov/2023/Sep/28/2003310132/-1/-1/0/CSI_PROCUREMENT_ACCEPTANCE_TESTING_GUIDE.PDF

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

ODNI, n.d.-a, "Safeguarding Science Goals", https://www.dni.gov/index.php/safeguarding-science

ODNI, n.d.-b, Supply Chain Risk Management for Industry & Academia, https://www.dni.gov/index.php/safeguarding-science/supply-chain-risk-management

OWASP, n.d., OWASP CycloneDX https://owasp.org/www-project-cyclonedx/