THE PRESIDENT'S NATIONAL SECURITY
TELECOMMUNICATIONS ADVISORY COMMITTEE

DRAFT NSTAC REPORT TO THE PRESIDENT

Measuring and Incentivizing the Adoption
of Cybersecurity Best Practices

Date: TBD

Table of Contents

Executive Summary

The U.S. national security posture depends on the secure, reliable functioning of our nation's critical infrastructure. However, the continued drumbeat of significant cyber incidents suggests existing market forces may be insufficient to incentivize the adoption of cybersecurity best practices and standards at the level needed to meet the evolving cyber-threat landscape and strengthen U.S. national security and emergency preparedness across some sectors. This includes best practices in both operational security and secure development and design.

Accordingly, the National Security Telecommunications Advisory Committee (NSTAC) was tasked with recommending ways to incentivize cybersecurity best practices, reduce barriers to their implementation, and measure best-practice adoption.

It is worth noting that market incentives to invest in cybersecurity do exist, and these incentives have resulted in proactive cybersecurity investments in many sectors. Consequently, cyber-attacks more often require greater technical expertise and infrastructure investments by malicious actors. However, part of the challenge is that market forces are not designed to reach a level of cybersecurity commensurate with goals of the administration and NSTAC with regard to national security and emergency preparedness. The gap between what markets naturally provide and what national security and emergency preparedness require is increasingly problematic. Nation-states are ramping up attacks on critical infrastructure that is developed, deployed, and managed by the private sector. This report focuses on how the United States can close the gap between critical infrastructure's current preparedness against cyberattacks and the evolving threat; how the United States can measure that gap; and how the United States can identify market factors, business models, and other issues that help or hinder cyber defense.

Report Focus and Scope

In developing this report, NSTAC received briefings from subject-matter experts representing government, critical-infrastructure industries, cyber-insurance providers, think tanks, and cybersecurity technology providers, as well as those specializing in measurements and metrics studies. NSTAC felt it was important to hear about the challenges and experiences organizations encounter when implementing and assessing the effectiveness of cybersecurity programs. Through expert briefings and NSTAC deliberations, NSTAC identified incentives for the adoption of cybersecurity best practices, as well as ways to measure the adoption of these best practices for both government and industry. In this report, NSTAC makes associated recommendations to the president for government policy to improve the adoption of cybersecurity best practices through the effective deployment of incentives and the use of stronger measurement and metrics.

Summary of Priority Findings and Recommendations

While the report includes multiple strategic findings and associated recommendations, NSTAC has highlighted here four critically important findings and associated recommendations for the president to implement, which will have the greatest impact.

Finding: In some cases, material gaps exist between the cybersecurity investments organizations make based on cost/benefit analysis and other risk-management considerations and the investments the federal government believes are required by those organizations to improve the security posture of the nation. Organizations that lack sufficient resources for cybersecurity investments, or for which market forces do not adequately incentivize cybersecurity investments at the level needed to ensure national security or emergency preparedness, will require additional incentives and support from the federal government to implement cybersecurity best practices.

Recommendation: *Economic Incentives.* Create and implement new market-based economic incentives for all commercial organizations to invest in cybersecurity best practices.

- The president should direct the Office of the National Cybersecurity Director (ONCD) to develop a strategy, in collaboration with government and industry stakeholders, to make recommendations on impactful financial incentives such as tax deductions or federal grants for organizations that adopt appropriate cybersecurity best practices that help adequately close the national security and emergency preparedness gap. The president should ask Congress for any authorities necessary to implement the recommendations of this strategy.

- The president should direct the ONCD to coordinate with relevant federal agencies, including the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Department of Defense, and the National Institute of Standards and Technology (NIST) to develop a nationwide education and outreach program targeted at critical-infrastructure providers—especially resource-poor small and medium-sized businesses—to significantly increase the use of the many free services offered by each agency, such as the CISA Cyber Hygiene Service and other shared cybersecurity-services programs, NSA Cyber Collaboration Center services, and NIST National Cybersecurity Center of Excellence programs. The president should direct the Office of Management and Budget (OMB) to ensure that future annual budget requests also adequately support the expansion of these programs.

Finding: Civil, criminal, and regulatory liability, as well as reputational challenges, create significant disincentives for effective cybersecurity information sharing; entities will require liability protections to participate in effective information-sharing processes, and any limits on liability must be clearly expressed.

Recommendation: *Risk Mitigation.* Re-imagine, create, and implement liability reforms that better align cybersecurity risk to business risk.

- The president should direct ONCD to develop a strategy, in coordination with the Department of Justice and other federal agencies and private sector stakeholders, to tie liability reform and safe harbors, using clearly defined and unambiguous language, to the sharing of cyber threat, incident, and other information with the government by organizations that can demonstrate they have adopted cyber best practices; where needed, the president should request authority from Congress

to implement the recommendations of this strategy prior to the expiration of the Cybersecurity Information Sharing Act of 2015.

Finding: Industry stakeholders have expended considerable efforts to align operational cybersecurity programs with the NIST Cybersecurity Framework (CSF) and other international, consensus-driven standards. However, duplication or conflict of regulatory requirements, including those from federal, state, local, territorial, tribal, global, and industry entities, continue to exert significant strain on organizational cybersecurity budgets, resources, and priorities.

Recommendation: *Regulatory Simplification.* Anchor all cybersecurity best-practice requirements to the most recent NIST CSF version.

- The president should direct OMB and the Office of Information and Regulatory Affairs to require federal agencies to conduct and publish a mapping of any new proposed cybersecurity requirements to the NIST CSF 2.0 and its successor versions in advance of the issuance of any new requirements. Deviations from the NIST CSF should be accompanied with an explanation for the necessity thereof, including an explanation of how such deviations were minimized to the greatest extent reasonably possible.

Finding: The government and private sectors have access to significant amounts of cybersecurity data that could be utilized to help support more effective measurements/metrics.

Recommendation: *Treat Cyber Statistics Like Economic Statistics.* Establish a Cybersecurity Measurement Center of Excellence within the Department of Commerce (DOC).

a. The president should authorize the establishment of a Cybersecurity Measurement Center of Excellence under the DOC to coordinate management and assessment of existing data sources across federal departments and agencies. The Center should bring together domain-knowledge experts from CISA and NIST with data-science experts from NIST and statistical experts from the DOC. The National Science Foundation (NSF) Secure and Trustworthy Cyberspace (SATC) program, or other appropriate government entities, can be used to assess existing, siloed data sources and how these existing data sources can help the federal government address economic and cybersecurity measurements.

1. Introduction

Background

The connected nature of cyberspace makes cybersecurity a shared responsibility of all ecosystem users. Effective cybersecurity thus requires complex interaction between public and private organizations with different—potentially conflicting—missions, perspectives, and resources. However, all organizations share a common goal of promoting cybersecurity and reducing cyber threats. Governments, standards organizations, and other stakeholders have created a plethora of cybersecurity best practices, but a significant number of critical-infrastructure organizations remain unaware of their existence, are not adopting them, or are poorly implementing them, resulting in uneven cybersecurity effectiveness. As cyberspace has become more reliable, its overall size has also increased with more stakeholders joining the ecosystem. Simultaneously, market concentration in some subsectors has increased the impact of successful attacks. This has caused U.S. government officials to raise concerns that extant market forces may be insufficient to incentivize the adoption of these best practices at the necessary level to combat the evolving cyber threat and secure U.S. national security and emergency preparedness interests.

The dynamic where point-source security solutions are developed anew for each emerging threat creates a challenge to identify effective operational strategies that are effective over time. In turn, this undermines the ability to systematically collect data about which practices work, which then challenges our ability to drive adoption of those practices across the economy—or even across critical segments upon which U.S. national security depends.

Critical infrastructure comprises 16 industry sectors of assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on U.S. national security, national economic security, and/or national public health or safety. The cyber threat to critical infrastructure is increasing and represents one of the most serious national security challenges the United States must meet. For example, according to research by Microsoft Corp., attacks targeting open-source software have grown on average 742 percent since 2019. Further, human-operated ransomware attacks are up more than 200 percent. Additionally, password-based attacks per month increased tenfold from April 2022 to April 2023.[1]

To counter this increasing threat environment, the spend on cybersecurity solutions and the corresponding size of the cybersecurity market has increased from $3.5B in 2004 to an estimated $1.75T over the five-year period from 2021-2025.[2] However, these investments are not uniformly distributed across the

[1] Microsoft. “Microsoft Digital Defense Report Building and improving cyber resilience.” October 2023. https://go.microsoft.com/fwlink/?linkid=2249025&clcid=0x409&culture=en-us&country=us

[2] Cybercrime Magazine. “Global Cybersecurity Spending To Exceed $1.75 Trillion From 2021-2025.” September 10, 2021. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

ecosystem. For example, publicly traded companies are more likely to invest in cybersecurity due to positive return in stock price.[3] By contrast, companies held by private equity may underinvest.[4]

In recent years, the failure to adopt cybersecurity best practices, including basic cyber-hygiene practices by poorly resourced and less mature organizations, have led to more successful cyberattacks on critical infrastructure, including the Colonial Pipeline and SolarWinds incidents. Complicating the adoption of best practices to combat cyber threats is the fact that cybersecurity capabilities, authorities, and responsibilities are highly distributed across the ecosystem. No single stakeholder can tackle the problem alone; progress is only possible in an environment where incentives exist to facilitate the adoption of cybersecurity best practices by all connected parties and that enable stakeholders to work together to combat cyber threats.

Although specific cybersecurity best practices vary by industry, risk tolerance, and other factors, several common themes emerge:

Data management and protection are paramount. Government agencies possess a great deal of critical infrastructure cybersecurity data from both public and private sector sources. For the government to realize the analytical benefits of this data, it must have a strong understanding of what this data is, where it resides, how it can be analyzed, and how it might contribute to more effective measurements and metrics. Care should be taken to protect stakeholders' data. If handled improperly, information about an organization's cybersecurity posture could be a roadmap for attackers.

Objective is better than subjective. Measurements should be quantitative rather than qualitative where possible, and methodologies should be transparent. Stakeholders deserve a clear understanding of how measurements are calculated and what steps can be taken to improve them. Likewise, effective measurements must reference the threat they are measured against. For example, effective mitigation against a criminal actor may be wholly ineffective against a nation-state actor. Measurements are inherently reductive and must be evaluated in context of a specific outcome.

Organizations respond better to carrots than sticks. To improve cybersecurity outcomes, an environment of "radical transparency" must be fostered in which organizations feel empowered and protected to share information with the federal government even when such information does not paint the entity in a good light. While regulatory punishments can drive compliance, they do so at the cost of causing the private sector to view the government as an additional adversary rather than a strong ally. Complementing required regulatory "sticks" with voluntary "carrots" offers several benefits, including fostering more nimble processes for tailoring cyber defenses to evolving threats, advancing business outcomes through more streamlined regulatory interactions, and fostering trust between the public and private sectors.

---

[3] Securities and Exchange Commission. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." March 9, 2022. https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf

[4] The Big Newsletter. "How to Get Rich Sabotaging Nuclear Weapons Facilities." January 3, 2021. https://www.thebignewsletter.com/p/how-to-get-rich-sabotaging-nuclear

Too many unprioritized requirements are counterproductive. The increasing regulatory burden on stakeholders presents effective compliance and oversight challenges, and it invites suboptimal outcomes. Regulatory harmonization and other deconfliction efforts are extremely important to drive more effective adoption of optimal best practices while reducing the burden of cybersecurity compliance, especially on small businesses.

Dramatically improving the adoption of best practices in cybersecurity requires a focus on people, processes, technology, business models, and governance. Success in each area demands sustained action by individuals and organizations, and the approaches and solutions must be scalable so that developers and operators can readily adopt them.

This report examines how positive and negative incentives influence individual and organizational decisions around cybersecurity investments, and it provides recommendations for the U.S. government to incentivize the adoption of cybersecurity best practices in a scalable, repeatable manner and facilitate better adoption and measurement of these best practices within organizations.

The Need for Cybersecurity Best-Practice Adoption

Critical infrastructure and other organizations should adopt multiple best practices to defend against cyber threats and should diversify their adoption to avoid relying on any single technology or strategy. Organizations should focus first on the basics: improving password hygiene and management, preventing social engineering-based attacks through awareness and other strategies, and patching known vulnerabilities.

Failure to adopt even one of these practices—for example, patching known vulnerabilities—can impact national cybersecurity posture: In April 2023, a joint governmental advisory from U.S. and U.K. cybersecurity agencies warned that poorly maintained network routers were subject to widespread attacks by a Russian state-sponsored Advanced Persistent Threat (APT) group[5]—despite the vendor having disclosed and patched the vulnerability in 2017 and warned of active exploit in 2018.[6] A similar dynamic occurred a few months later. In June 2023, the Cybersecurity and Infrastructure Agency (CISA) directed all federal civilian agencies to turn off web-user interfaces for networked management interfaces[7]—warnings of this type also send a powerful signal to network administrators globally. But months later, tens of thousands of web-facing network management devices were found vulnerable to attack via this same pathway.[8]

Another important area of focus is improving credential and access management since credential-focused attacks remain among the most frequent causes of breaches. Bad actors can gain access to critical networks using stolen or weak credentials due to lax password requirements, password re-use, use of default passwords, or even a lucky brute force attack. For example, in a recent cluster of incidents, Unitronics programmable logic controllers (PLCs) were mistakenly left facing the internet with weak or default passwords, and hackers used those credentials to take control of municipal water and wastewater systems.[9]

Finally, it is critical to educate employees and customers to defend against the growing deluge of social-engineering attacks, of which phishing and pretexting are the most common. A recent high-profile social engineering-driven breach involved Las Vegas casinos, such as MGM and Caesars Palace, where the threat actor Scattered Spider used social engineering to convince IT help desk personnel to reset passwords and/or multi-factor authentication tokens.[10] Implementing best practices to protect against attack vectors that leverage human psychology and vulnerability must be a basic cornerstone of cyber defense.

---

[5] National Cybersecurity Center. "APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers." April 18, 2023. https://www.cisa.gov/sites/default/files/2023-04/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers-uk.pdf

[6] https://blog.talosintelligence.com/state-sponsored-campaigns-target-global-network-infrastructure/

[7] Cybersecurity and Infrastructure Security Agency. "CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities." October 23, 2023. https://www.cisa.gov/news-events/alerts/2023/10/23/cisa-updates-guidance-addressing-cisco-ios-xe-web-ui-vulnerabilities

[8] The Economic Times. "Tens of Thousands of Cisco Devices Compromised After Hackers Exploit Critical Bug." October 20, 2023. https://telecom.economictimes.indiatimes.com/news/devices/tens-of-thousands-of-cisco-devices-compromised-after-hackers-exploit-critical-bug/104582658

[9] Cybersecurity and Infrastructure Security Agency. "Exploitation of Unitronics PLCs used in Water and Wastewater Systems." November 28, 2023. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

[10] Cybersecurity and Infrastructure Security Agency. "Cybersecurity Advisory: Scattered Spider." November 16, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

Table of Findings and Recommendations

Finding #	Finding	Recommendation	Responsible Entity
I	In some cases, material gaps exist between the cybersecurity investments organizations make based on cost/benefit analysis and the investments the federal government believes are required to improve the security posture of the nation.	Develop a strategy to make recommendations on impactful financial incentives for organizations that adopt appropriate cybersecurity best practices.	Office of the National Cybersecurity Director (ONCD)
		Develop a nation-wide education and outreach program to significantly increase the use of the many free services offered by government agencies.	ONCD, CISA, National Security Agency (NSA), Department of Defense (DoD), National Institute of Standards and Technology (NIST)
		Develop a unified set of cybersecurity requirements for procurement.	Office of Management and Budget (OMB), ONCD
		Identify existing disincentives and barriers to adoption of vendor-supplied patches and secure configuration guidance.	ONCD, CISA, General Services Administration (GSA)
		Develop sample Request for Proposal (RFP) language addressing cybersecurity requirements for critical infrastructure organizations using third-party products or services.	CISA
II	Civil, criminal, and regulatory liability create extreme disincentives for effective cybersecurity information sharing.	Develop a strategy to tie liability reform and safe harbors to the sharing of cyber threat, incident, and other information with the government.	ONCD, Department of Justice (DOJ)
		Ensure that liability protections afforded to entities that report cyber-incident information to the government under the Critical Infrastructure Act of 2022 (CIRCIA) information-sharing rules are harmonized with the liability protections of the Cybersecurity Information Sharing Act of 2015.	CISA
		Establish a clear mechanism to anonymize and remove attribution for any cyber threat or incident information that has been shared with a government agency.	ONCD
		Provide clear mandates to federal departments and agencies that any limits on liability that they are offering to private sector organizations must be clearly defined and delineated.	OMB, ONCD, CISA, DOJ

III	Duplication/conflict of regulatory requirements (federal; state, local, tribal, territorial (SLTT); global; industry) continue to exert significant strain on organizational cybersecurity budgets, resources, and priorities.	Require federal agencies to conduct and publish a mapping of any new proposed cybersecurity requirements to the NIST Cybersecurity Framework (CSF) 2.0 and its successor versions.	OMB
		Require the use of a single, repeatable set of requirements, aligned with the NIST CSF for use in existing and future federal cybersecurity grant programs.	ONCD, CISA, OMB
		Accelerate implementation of the NSTAC Enhancing Internet Resilience Phase IV recommendations on regulatory alignment.	White House
IV	The government and private sectors have access to significant amounts of cybersecurity data that could be utilized to help support more effective measurements/metrics.	Establish a Cybersecurity Measurement Center of Excellence under the Department of Commerce to coordinate data collection and management.	Department of Commerce (DOC)
		Develop a data management roadmap to prepare for implementation of CIRCIA and to leverage anonymized data received from the National Cyber Security Review (NCSR).	CISA
V	Cybersecurity measurements that are tied to business outcomes will be more effective	Develop a resource center to help organizations leverage NIST CSF 2.0 to develop measurements and metrics tied to business outcomes.	NIST, CISA
VI	Strengthening the nation's cybersecurity depends on the ability of public and private sector decision makers to make risk-informed decisions	Produce a study to determine differences between business risk tolerance based on economics and societal and national security risk tolerance.	ONCD, CISA, National Security Council (NSC), National Economic Council (NEC), DOC
VII	Subjective measurements, combined with bad math, lead to ineffective decision making	Develop a methodology for assessing cybersecurity measurements using existing cybersecurity survey data.	NIST
		Develop a methodology and mechanisms to assess the performance of measurement methods.	NIST, CISA
		Develop material to educate and encourage organizations to adopt more quantitative risk management strategies.	NIST, CISA
VIII	Private firms may hold data that can serve as a proxy to measure best-practice adoption.	Study whether firms, such as cyber insurance companies, have information/data that could help assess the state of best-practice adoption and the impact of cyber insurance on best-practice adoption.	DOC

		Provide a recommendation on expected effects of a cyber insurance backstop relative to insurance industry capital responsiveness.	Department of Treasury
		Evaluate the effects of categorical insurance exclusions and respective impacts to critical infrastructure and national security and emergency preparedness risk exposure.	ONCD, CISA, DoD
IX	Lack of qualified personnel is consistently cited as both a barrier to adoption of best practices and a barrier to effective cybersecurity measurement.	Establish virtual national cyber academies to provide free training in exchange for service.	ONCD, DoD, CISA, NIST, National Science Foundation (NSF)
		Promote best practices for people-based cyber resilience training based on the National Initiative for Cybersecurity Education (NICE) Framework.	NIST, Department of Education, Department of Labor (DOL), CISA
		Develop guidance for public and private sector organizations to utilize competency-based hiring to fill workforce gaps.	Office of Personnel Management (OPM), DOL
		Develop a strategy to mobilize cybersecurity experts, including retired computer security professionals, to support a "Cyber Corps" to assist small businesses.	ONCD
X	Phased approaches to secure software-development requirements can strengthen outcomes.	Seek guidance or standards from the private sector to develop reasonable compliance timeframes for the OMB/CISA Secure Software Self-Attestation Common Form.	CISA
		Seek private sector-developed maturity-model guidance or standards that can be applied to the Secure Software Development Framework.	NIST
		Create a Grand Challenge on how the federal government can incentivize the creation of resources designed to improve the quality and security of open-source software without impacting innovation.	NIST, CISA
XI	Public and private sector organizations should be encouraged to leverage effective technologies that give defenders an advantage.	Create a Cybersecurity Grand Challenge for organizations to leverage next generation AI/ML capabilities to more effectively drive adoption and use of cybersecurity best practices and enable more efficient measurement of their use.	ONCD, CISA, NIST, Department of Education
		Identify highly effective security use cases for AI/ML systems and publish automation templates and accompanying documentation.	CISA
XII	A healthy security workplace culture is a leading indicator of strong cybersecurity.	Conduct a study on how best to measure and track progress toward healthy security culture.	National Academy of Sciences

2. Findings and Recommendations

Part I – Incentives Are Required to Achieve National Security Goals

Finding: In some cases, material gaps exist between the cybersecurity investments organizations make based on cost/benefit analysis and other risk-management considerations and the investments the federal government believes are required by those organizations to improve the security posture of the nation. Organizations that lack sufficient resources for cybersecurity investments, or for which market forces do not adequately incentivize cybersecurity investments at the level needed to ensure national security or emergency preparedness, will require additional incentives and support from the federal government to encourage adoption of cybersecurity best practices.

- **Priority Recommendation:** The president should direct ONCD to develop a strategy, in collaboration with government and industry stakeholders, to make recommendations on impactful financial incentives, such as tax deductions or federal grants, for organizations that adopt appropriate cybersecurity best practices that help adequately close the national security and emergency preparedness gap. The president should ask Congress for any authorities necessary to implement the recommendations of this strategy.

- **Priority Recommendation:** The president should direct ONCD to coordinate with relevant federal agencies, including CISA, NSA, DoD, and NIST to develop a nation-wide education and outreach program targeted at critical infrastructure providers, especially resource-poor small and medium-sized businesses, to significantly increase the use of the many free services offered by each agency, such as the CISA Cyber Hygiene and other shared cybersecurity services programs, NSA Cyber Collaboration Center services, and NIST National Cybersecurity Center of Excellence (NCCOE) programs. The president should direct OMB to ensure that future annual budget requests also adequately support the expansion of these programs.

The public and private sectors appropriately assess risk in different ways. For the private sector, risk is primarily an economic issue—security is largely funded at a per-entity, commercial level, and therefore the private sector will invest in cybersecurity at levels commensurate with economic and business risk. The government has extra-economic issues, most notably regarding national security, economic security, and emergency preparedness. This difference leads to a delta between what the government and private sector view as optimal cybersecurity investments.

As a result, there is a need for additional incentives to motivate private sector actors to invest in cybersecurity best practices at a level deemed sufficient by the government to ensure its national security and other extra-economic priorities are met.

Different types of incentives (enabling and motivating) may be more appropriate depending on the maturity or resources of the entity they are targeted towards. Enabling incentives are those that help a less mature organization get off the ground. Motivating incentives are those that encourage investment by larger organizations with established cybersecurity programs.

Distinct incentives across different sectors may alternatively drive or hinder investments in cybersecurity. Prior research in cybersecurity economics has documented the following disincentives and incentives:

1. Disincentives[11]:

    a. **Inability to Understand Return on Investment (ROI):** Consumers, unable to distinguish between secure and insecure products, may be unwilling to pay for security and thus disincentivize organizations from associated investment. Until a security incident occurs, there also may be a significant problem in appreciating the value of investments intended to stave off an event that has never happened before—and may never happen in the future. Effective security investments may compound the complexity of calculating the ROI by preventing events which are then never experienced and whose costs are then hard to tally.

    b. **Externalized Risk:** The consequences of certain cybersecurity threats, such as Internet of Things (IoT) botnets, may not be borne by either the manufacturer or the customer. Instead, they are borne by the victim of the distributed denial-of-service attacks. Since the customer is often not impacted, they may be unwilling to pay for a more secure IoT device; consequently, the manufacturer is incentivized to control costs due to price competition and include no more security than consumers will differentiate and be willing to pay for rather than to build and maintain products that are secure by design.

    c. **Lock In:** Adding security features and functionality may add not only cost but time to the development process for new products. Therefore, vendors may limit security efforts in their rush to be first to market. And once users embrace a first-to-market product, it may be costly to switch to a more security-focused vendor.

    d. **Ownership:** Certain ownership structures, such as start-ups and private equity, may also under invest in cybersecurity as they may prioritize short-term profits over long-term risk management.

    e. **Hidden Lifecycle Cost of Unsecure Technology:** There may be significant benefits in terms of reducing or more effectively managing cybersecurity risk that come from applying patches, adopting secure configurations, retiring equipment that is end of support, or even uplifting on-premises resources to the cloud where security functions can essentially be outsourced to organizations with dedicated security 24/7 capabilities. However, each of these decisions comes with significant costs. Frequently these come in the form of ongoing operational expenses that fail in comparison to what seems to be a "cost-free" option to maintain the status quo. There is no current mechanism to ensure that these shadow, off-book "security debts" are accounted for when assessing and comparing costs of options to buy down security risk. This results in market

[11] Anderson, R. and Moore, T., 2006. The economics of Information Security. Science, 314(5799), pp.610-613.

failure—particularly when combined with other forces listed above, including externalization of costs or other negative incentives to address security risk.

f. **Point-Sourced Cybersecurity Solutions:** Cybersecurity solutions are often very point-sourced—they are often the result of a start-up who innovates to solve a specific new security threat. As a result, companies seeking to protect their enterprises often rely on a panoply of specific solutions from a wide array of vendors. The complexity of ingesting and managing data across these various security vendor solutions and the increasingly multi-cloud-based environments used to store and manage data and applications is outstripping the capabilities of even well-resourced sophisticated enterprises and governments—not to mention small and medium-sized commercial enterprises, SLTT governments, academic institutions, civil society, etc. The absence of either sufficient numbers of trained security professionals or mechanisms to scale and automate efforts to draw insights about anomalous cyber activity and action responses is a serious barrier to effectively securing our nation's security future.

2. Incentives[12]:

a. **Competitive Advantage:** Many businesses have specific IP or other proprietary information that gives them a competitive advantage. Organizations may invest in cybersecurity to protect this advantage. Companies can also use cybersecurity as a competitive differentiator. For example, the U.S. government has announced the implementation of a voluntary cybersecurity labeling program for IoT devices that have been developed with certain security features and defaults-built in.[13] A labeling program has the potential to help consumers differentiate between IoT devices with built-in security features and those that lack these features, which could be effective if consumers understand and value the included security features that the label represents.

b. **Reputation and Branding:** A cybersecurity incident may harm the reputation of an organization leading to a reduction in stock price. This reputational harm may be more salient for organizations that differentiate their products on security. In addition, disproportional coverage of a security issue in the media may create board-level pressure to invest in specific solutions. Organizations may thus invest in cybersecurity to maintain their reputation and differentiate their brand (on cybersecurity).

c. **Reduce Operational Costs and Business Risk:** Reduction in operational costs, such as insurance, as well as the risk of business disruption by threats like ransomware, may further cybersecurity

[12] Garg, V., 2021, July. Covenants Without the Sword: Market Incentives for Cybersecurity Investment. In TPRC49: The 49th Research Conference on Communication, Information, and Internet Policy.

[13] Federal Communications Commission. "FCC Proposes Cybersecurity Labeling Program for Smart Devices." August 10, 2023. https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device.

investment. Further, investments in cybersecurity can help prevent other added costs in terms of post-incident cleanup, additional hiring, customer notification, and more.

d. **Business Enabler:** Certain cybersecurity investments may help organizations get access to additional markets, e.g., Federal Risk Authorization Management Program (FedRAMP) for the U.S. government's cloud-related needs.

Short-term budget requirements often impede cybersecurity investments, whereas the need to reduce risk and enable business promotes it. These competing dynamics have largely driven an increase in the cybersecurity market at a cumulative average growth rate of over 20 percent. However, these investments may not be spread uniformly across all organizations. For example, small and medium-size businesses may find cybersecurity investments to be prohibitively expensive.

There may be differences even across organizations that may make investments. For example, a desire for risk transfer may drive investment in third-party technologies rather than in-house, first-party development. Some organizations may prioritize the business advantage of meeting a presumed standard of due care based on existing case law to avoid ex-post penalties, rather than technical merits when deploying specific security controls. This may result in centralization of risk in specific vendors or technologies, potentially increasing the impact of any future incidents.

In addition to free market incentives, additional incentives may be created by government or private sector action. Previous government reports have noted various cybersecurity-related incentives[14,15], including 1) creating an expedited security clearance process, 2) providing federal funding for framework adoption, 3) including cybersecurity in rate base, 4) retaining real-time information sharing, 5) allowing cyber insurance, 6) limiting ex-post liabilities and ex-ante obligations, 7) limiting regulatory requirements, 8) prioritizing technical assistance, 9) giving preference in federal procurement, 10) delivering public recognition, 11) preventing public disclosure, 12) streamlining regulations, 13) providing subsidies, and 14) providing tax incentives.

U.S. government agencies currently provide multiple free services to help organizations achieve baseline cybersecurity hygiene practices and to share information on cybersecurity threats and best practices. CISA provides Cyber Hygiene services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.[16] The NSA offers organizations an opportunity to engage at the Cybersecurity Collaboration Center to scale intel-driven cybersecurity through open, collaborative partnerships to harden the U.S.

---

[14] National Telecommunications and Information Administration. "Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program." August 16, 2013. https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf

[15] Cybersecurity and Infrastructure Security Agency. "Executive Order 13636: Improving Critical Infrastructure Cybersecurity." June 12, 2013. https://www.cisa.gov/sites/default/files/publications/19_1115_dhs-eo13636-analytic-report-cybersecurity-incentives-study%281%29.pdf

[16] Cybersecurity and Infrastructure Security Agency. "Cyber Resource Hub." https://www.cisa.gov/cyber-resource-hub

Defense Industrial Base.[17] DoD's Under Advisement program is a U.S. Cyber Command portal for information sharing to and from private-sector partners.[18] And the NIST National Cybersecurity Center of Excellence is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges.[19]

While each of these programs provide valuable cybersecurity services to critical infrastructure and other organizations, briefers to the President's National Security Telecommunication's Committee (NSTAC) have noted that the services are not widely utilized at a national scale. Further, there may be confusion about the differences between the multiple services and which might be most appropriate for different stakeholders. These programs would benefit from greater outreach and clarity.

The NSTAC makes the following additional recommendations on incentives:

- **Recommendation:** The president should direct OMB, in coordination with ONCD, and other relevant federal entities to develop a unified set of cybersecurity requirements for procurement (leveraging existing government procurement programs and/or international standards) to drive both stronger adoption of cybersecurity best practices and regulatory harmonization).

- **Recommendation:** The president should direct ONCD, in coordination with CISA and the GSA FedRAMP Program Management Office, to consult with private sector stakeholders to identify existing disincentives and barriers to adoption of vendor-supplied patches and secure configuration guidance that address critical vulnerabilities and known exploited vulnerabilities and to encourage software manufacturers to incorporate those learnings into their secure-by-design programs.

- **Recommendation:** The president should direct CISA to work with critical-infrastructure sector coordinating councils to develop sample RFP language addressing cybersecurity requirements for critical infrastructure organizations using third-party products or services. The sample language should be shared publicly for voluntary use by any organization, especially a small or medium-size business, and should be updated regularly.

Part II – Liability Protection Supports Effective Information Sharing

Finding: Civil, criminal, and regulatory liability create extreme disincentives for effective cybersecurity information sharing; entities will require liability protections to participate in effective information-sharing processes, and any limits on liability must be clearly expressed.

---

[17] National Security Agency. "Cybersecurity Collaboration Center." https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/

[18] U.S. Cyber Command. "Private Sector Partnerships." https://www.cybercom.mil/Partnerships-and-Outreach/Private-Sector-Partnerships/

[19] National Telecommunications and Information Administration. "National Cybersecurity Center of Excellence." https://www.nccoe.nist.gov/

- **Priority Recommendation**: The president should direct ONCD to develop a strategy, in coordination with DOJ and other federal agencies and private-sector stakeholders, to tie liability reform and safe harbors, using clearly defined, unambiguous language, to the sharing of cyber threat, incident, and other information with the government by organizations that can demonstrate they have adopted cyber best practices; where needed, the president should request authority from Congress to implement the recommendations of this strategy prior to the expiration of the Cybersecurity Information Sharing Act of 2015.

Many private-sector cybersecurity teams opt not to share cyber threat intelligence (CTI) and other related information that could potentially help business partners, supply chain partners, vendors, industry peers, critical infrastructure operators, and public-sector actors, even when they have good relationships with such organizations and institutions. There are several factors that contribute to this behavior.

Sharing or disclosing CTI to third parties can be interpreted as an admission or even an announcement that an organization has suffered a data breach or is in the process of investigating a cybersecurity incident. When private-sector organizations, other than cybersecurity firms themselves, share information on new indicators of compromise or novel attack tactics, this can trigger public speculation that the sharing party collected such information as part of an internal data breach investigation. The hint of such potentially negative news is enough to stoke broad industry speculation and lead to public victim shaming. This can generate negative news cycles, tarnish private-sector organizations' brands, and impact publicly traded companies' short-term equity values. Such news can also tarnish the careers of senior cybersecurity managers, Chief Information Security Officers, and other C-level executives. Subsequently, the General Counsels of many private-sector firms have concluded that keeping such information strictly confidential and disclosing only what is required by law minimizes potential legal and public-relation risks and reduces exposure to potential negative regulatory outcomes.

To foster an environment where information sharing processes can function more effectively, organizations will require protections against regulatory and criminal liabilities, lawsuits, and other potential liabilities that often accompany cybersecurity incidents. Liability concerns create a real impediment to effective coordination of cybersecurity responses, including those from government and private-sector actors to disrupt or defend against malicious activity. Improving liability protections will enhance coordination between government and private-sector actors and enable targeted cyber threat-response approaches. Organizations will want to have confidence that any information they share will not be used against them for enforcement actions. Limits on liability must be clearly expressed. To these ends, NSTAC makes the following additional recommendations:

- **Recommendation:** The president should task CISA with ensuring that liability protections afforded to entities that report cyber-incident information to the government under the Cyber Incident Reporting for CIRCIA information-sharing rules are harmonized with the liability protections of the Cybersecurity Information Sharing Act of 2015.

- **Recommendation:** The president should direct ONCD to establish a clear mechanism to anonymize and remove attribution for any cyber threat or incident information that has been shared with a government

agency before it is further disseminated to other government agencies or from the government to private-sector entities.

- **Recommendation:** The president should task OMB, in partnership with ONCD, CISA, DOJ, and other government stakeholders, to provide clear mandates to federal departments and agencies that any limits on liability that they are offering to private-sector organizations must be clearly defined and delineated to minimize uncertainty and maximize program participation.

Part III – Overlapping/Conflicting Regulations Strain Resources

Finding: Industry stakeholders have expended considerable efforts to align operational cybersecurity programs with the NIST CSF and other international, consensus-driven standards. However, duplication/conflict of regulatory requirements (federal, SLTT, global, industry) continue to exert significant strain on organizational cybersecurity budgets, resources, and priorities.

- **Priority Recommendation:** The president should direct OMB and the Office of Information and Regulatory Affairs to require federal agencies to conduct and publish a mapping of any new proposed cybersecurity requirements to the NIST CSF 2.0 and its successor versions in advance of the issuance of the new requirements.

In February 2023, NSTAC published a report entitled "Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem." One of its findings stated, "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." Please see the table in Appendix A for examples of cybersecurity frameworks and associated requirements.

Many large and medium-sized private-sector organizations typically have multiple regulated and industry cybersecurity-related standards they must or should comply with. For example, publicly traded private-sector organizations that service consumers in the United States and internationally, and also seek to do business with the federal government, might need to comply with cybersecurity-related frameworks and standards as published by the NIST, the International Organization for Standardization (ISO), the Securities and Exchange Commission (SEC), the Defense Federal Acquisition Regulation Supplement (DFARS), and the Payment Card Industry (PCI), as well as state laws such as the California Consumer Privacy Act (CCPA), among others.

Many of these regulated and industry standards require organizations to implement and operate the same or similar cybersecurity controls. Duplication of regulated cybersecurity-related requirements and conflicts between such requirements cause significant confusion and strain on organizational cybersecurity budgets, resources, and priorities as they attempt to rationalize required investments for compliance. Very often, individual organizations' security and compliance teams are left to decide which cybersecurity controls to implement based

on which controls offer the least bad regulatory outcomes, instead of how controls appropriately mitigate associated cybersecurity risks.

The government has recognized this issue in its National Cyber Security Strategy, as well as its Request for Information on regulatory harmonization. Additionally, OMB recognized this burden in a draft memo released on October 27, 2023, regarding "Modernizing the Federal Risk Authorization Management Program (FedRAMP)."[20] The memo states, "[M]any existing cloud offerings have implemented or received certifications for external security frameworks. Performing an assessment of such a framework each time a product that uses it goes through the FedRAMP process unnecessarily slows the adoption of such cloud products and services by the federal government. Therefore, FedRAMP will establish standards for accepting external cloud security frameworks and certifications, based on its assessment of relevant risks and the needs of federal agencies."

Some examples of duplicative, conflicting, or confusing regulated cybersecurity requirements are listed in the table in Appendix A. These examples illustrate why there is confusion and lack of clarity across different cybersecurity standards. These examples highlight a relatively small number of the control categories from different popular cybersecurity-related frameworks and standards as published by NIST, SEC, DFARS, ISO, and PCI. The examples in the table that represent relatively stringent requirements are in emboldened text. This is not an exhaustive list, nor does it represent the scope of assets these requirements might need to be applied to. The inconsistency in how these requirements is stated as "must" versus "should" across standards and frameworks adds to the confusion. The control examples in the table in Appendix A cover the following control objectives:

a. **Access Reviews**: The intent is to establish a "regular" review process with a more stringent requirement of doing it annually. The regularity or frequency of running this process is often confusing or simply not defined.

b. **Incident Reporting:** The intent is to share information on very recent or nascent attacks that might help other potential victims. Requirements vary from having no specific timeline to reporting within 72 hours or filing within a timely manner (within a few days up to a week after an incident).

c. **Vulnerability Scanning**: The intent is to specify how often vulnerability scanning should be performed. Requirements specifying the frequency for performing vulnerability scanning are highly variable including "regular," quarterly, annually, risk-based, and when hardware or software changes occur. Very often clarity on scope is not included; for example, which assets need to be included—internal and/or external networks, web applications, information systems, ports, services, etc.

d. **Penetration Testing:** The intent is to specify when penetration testing should be conducted so that defenders can find exploitable vulnerabilities before attackers can find them. The frequency specified in

[20] The White House. "Office of Management and Budget Releases Draft Memorandum for Modernizing the Federal Risk and Authorization Management Program (FedRAMP)." October 27, 2023. https://www.whitehouse.gov/omb/briefing-room/2023/10/27/office-of-management-and-budget-releases-draft-memorandum-for-modernizing-the-federal-risk-and-authorization-management-program-fedramp/#:~:text=The%20proposed%20guidance%2C%20which%20would,Government.%20Development%20of%20the%20draft

standards for performing these scans is highly variable, including quarterly, annually, risk-based, or based on specific organizational plans developed.

e. **Log Preservation:** The intent is to specify how long log files should be stored before deletion so that they can be used in potential future incident-response investigations as needed. Retention periods specified in standards are either not defined or can extend up to six years.

f. **Encryption Strength:** The intent is to specify which modern encryption characteristics, such as the encryption algorithm and key lengths, are adequate to protect the confidentiality and integrity of organizations' data given current computational capabilities to defeat encryption controls. These vary from "no specific strength" to "appropriate strength" to specific key length values like 128 bits for data at rest and 192 bits for data in transit, to specific encryption algorithms and corresponding key lengths such as FIPS 140-2 compliant algorithms with AES 128-bit minimum and 256-bit for top-level protection.

Additional details are outlined in the table of Appendix A. Note that new requirements are frequently introduced to standards as they are updated, while older requirements are often updated as well.

The NSTAC makes the following additional recommendations:

- **Recommendation:** The president should task ONCD, in partnership with CISA and OMB, to require the use of a single, repeatable set of requirements aligned with the NIST CSF for use in existing and future federal cybersecurity grant programs.

- **Recommendation:** The federal government should accelerate implementation of the NSTAC Enhancing Internet Resilience Phase IV recommendations on regulatory alignment.[21]

Part IV – Leveraging Existing Cybersecurity Data

Finding: The government and private sectors currently have access to significant amounts of cybersecurity data that could be utilized to help support more effective measurements and metrics.

- **Priority Recommendation:** The president should authorize the establishment of a Cybersecurity Measurement Center of Excellence under DOC to coordinate data collection and management with federal departments and agencies. The Center should bring together domain-knowledge experts from CISA and NIST with data science experts from NIST, and statistical experts from DOC. The NSF SATC program, or other appropriate government entity, can be used to assess what data sources are available and to assess what economics questions could be addressed through those.

[21] 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. https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf

Data, especially sensitive cybersecurity data such as defensive measures, penetration test results, and other information that may expose an organization to risk, must be consumed and protected with the highest degree of integrity to maintain the trust and confidentiality of the data owner and the entity processing the data. To this end, the government must define clear specifications on how data is initially collected, and which organization(s) is authorized to collect specific data.

The NSTAC recommends that this start with the establishment of a Cybersecurity Measurement Center of Excellence within DOC and tasking it with establishment of publicly available documentation detailing exactly which organizations can gather cybersecurity data, exactly what data each organization may gather, and for what purpose the data is used. The defined specification should include existing methods for requesting and obtaining data between organizations, as well as establishing a centralized mechanism using standardized policies and processes for data sharing moving forward. Privacy considerations, such as anonymization of data and protection of data, must be addressed through internal rules governing the operation of the Center of Excellence.

Once guidelines are clearly defined regarding the collection, management, and protection of cybersecurity data, a collaboration between government and Industry should be used to define models for consumption of generated data. As data collected is expected to be a combination of both publicly available data as well as government and industry-provided data, the models should take into account existing regulations defined under the forthcoming CIRCIA, managed by CISA. The CIRCIA defines specific requirements placed upon the industry regarding the reporting of cyber incidents but does not specify the exact structure and extent of the data provided. Whatever models are generated should account for any specification defined by the CIRCIA rulemaking process. The handling and dissemination of the output of these models must be clearly defined and determined in conjunction with industry partners.

After defined policies and infrastructure are established for the collection and processing of data, it will be critical to provide incentives to both government and commercial entities to encourage the engagement. The committee recommends two specific forms of incentivization related to data collection and sharing. First, similar to recommendations made in Part I, organizations should be provided with incentives for providing open-source access or free-to-use licensing for older versions of tools and technologies related to data collection and/or processing. This will allow them to maintain their most advanced capabilities within their existing licensed products, while still obtaining notable benefits from the sharing of prior versions. Second, the administration should work with Congress to clearly define when those sharing information should be immune from civil and criminal liability or regulatory enforcement actions when sharing cybersecurity data.

The NSTAC makes the following additional recommendation:

- **Recommendation:** The president should task CISA with developing a data management roadmap to strategically prepare to ingest data through implementation of CIRCIA, leverage anonymized data received from the National Cyber Security Review (NCSR) through the Multi-State Information Sharing and Analysis Center (MS-ISAC) to be able to cross reference these data sets for insights, and disseminate appropriate cyber-threat and incident information to help critical infrastructure entities protect themselves.

Part V – Connecting Cybersecurity Metrics to Business Outcomes

Finding: Cybersecurity measurements that are tied to business outcomes will be more effective than those that are disconnected from the business; metrics should be tied to decision deliverables.

- **Priority Recommendation:** The president should task the director of NIST to work with the director of CISA and the private sector to develop a resource center to help organizations leverage the governance function of the NIST CSF 2.0 to develop measurements and metrics tied to business outcomes. This resource center should include business outcome-aligned guidance on adopting the NIST CSF 2.0, the CISA CPGs, the NCCOE practice guides, and the NIST Secure Software Development Framework (SSDF), among other resources. Following the release of CSF 2.0, CISA should update the CPGs to ensure alignment with the new functions, categories, and subcategories of the CSF.

Organizations and enterprises, including critical infrastructure providers, face significant challenges understanding which cybersecurity investments will be most effective in reducing risk. Organizational information technology and cybersecurity strategies and tactics developed independently from business goals and objectives can lead to misaligned investment incentives. In these cases, total cybersecurity spend may increase, but may not be optimally reducing business risk. Similarly, the use of measurements and metrics in a cybersecurity program can demonstrate how an organization is making progress towards achieving certain security outcomes. However, this progress may still leave an organization unduly exposed if these measurements and metrics are not tied to business outcomes. This is especially true when organizations are facing downward pressure on expenditures and must prioritize budget decisions.

According to research from Forrester in a 2020 online survey of more than 800 security and business executives, "fewer than 50% of security leaders are framing the impact of cybersecurity threats within the context of a specific business risk. Only half (51 %) say their security organizations work with business stakeholders to align cost, performance, and risk-reduction objectives with business needs. Four out of ten (43%) report they regularly reviewed their security performance metrics with business stakeholders."[22] Similarly, Cisco's Cybersecurity Readiness Index found that a mere 15 percent of the nearly 7,000 organizations surveyed globally were mature in their level of cyber-risk preparedness. This was despite that almost 60 percent of respondents reported having experienced a cybersecurity incident in the preceding 12 months.[23] Multiple briefers for NSTAC expressed the importance of aligning cybersecurity measurements and metrics to business goals and outcomes. Alignment can help organizations understand which assets are most important to business functions and establish programs and processes to prioritize the protection of these assets in a measurable way.

Multiple nonprofit, government, and other industry organizations are developing tools to help organizations link cybersecurity investments with business outcomes and return-on-investment data. As examples, NIST has

[22] Forrester. "The Rise Of The Business-Aligned Security Executive." August 2020. https://static.tenable.com/marketing/whitepapers/Forrester-The_Rise_Of_The_Business-Aligned_Security_Executive.pdf

[23] Cisco. "Cisco Cybersecurity Readiness Index." March 2023. https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

developed tools to help organizations better align their security functions with overall business-risk management.[24] The Factor Analysis of Information Risk Institute (FAIR) develops frameworks and tools to help organizations measure, manage, and report on information risk from a business perspective.[25]

Draft version 2.0 of the NIST CSF highlights the importance of communicating cybersecurity risk and posture for both internal and external stakeholders for an organization.[26] Version 2.0 includes a new governance function, which covers how an organization can make and execute its own internal decisions to support its cybersecurity strategy. It also provides guidance on how organizations can integrate cybersecurity risk-management practices into their overall enterprise risk-management practices. The CSF enables different organizations, across different industries and with different resources and risk tolerances, to utilize a common language to communicate how they can move from their current cybersecurity postures to desired cybersecurity states in a measurable way.

The NIST NCCOE develops both sector-specific and cross-sector guidance to address discrete cybersecurity challenges faced by different sectors. It develops comprehensive practice guides and reference architectures, leveraging lab-based integrations of commercially available software solutions from a range of industry partners.

CISA has developed the Cross-sector Cyber Performance Goals (CPGs), which are aligned with the NIST CSF, to provide a baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.[27] CISA has positioned the CPGs as a steppingstone for less mature critical infrastructure owners and operators to begin their journey toward full adoption of the NIST CSF. CISA has developed a CPG checklist for organizations to assess and document their adoption of the various controls included in the CPGs.[28] The checklist serves as the basis for an entity to utilize cybersecurity metrics.

The CSF, the CPGs, and the NCCOE practice guides are valuable tools designed to help organizations reduce cybersecurity risk. However, each resource requires individual organizations to evaluate their risk assessments and tailor their cybersecurity programs for their respective environments. This can be more challenging for less mature organizations, many of whom are owners and operators of critical infrastructure and are building or growing their cybersecurity programs from baseline levels.

Articulating the links between cybersecurity practices and business outcomes is critical for these entities. NIST and CISA have an opportunity to work closely with industry and other stakeholders to develop and promote

---

[24] National Telecommunications and Information Administration. “Integrating Cybersecurity and Enterprise Risk Management (ERM).” October 2020 https://csrc.nist.gov/pubs/ir/8286/final

[25] FAIR Institute. https://www.fairinstitute.org/

[26] National Telecommunications and Information Administration“ https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

[27] Cybersecurity and Infrastructure Security Agency. “Cross-Sector Cybersecurity Performance Goals.” July 21, 2023. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[28] Cybersecurity and Infrastructure Security Agency. “CISA CPG Checklist.” March 2023. https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

guidance that makes it easier for organizations to effectively utilize these resources and to better understand how they can tie their cybersecurity programs to their business outcomes.

Part VI – Understanding the Gap Between Economic and National Security Risk Tolerance

Finding: Strengthening the nation's cybersecurity depends on the ability of public and private sector decision makers to make risk-informed decisions on the most effective solutions available when allocating limited resources. More support is needed from the federal government to achieve these goals.

- **Priority Recommendation:** The president should direct ONCD, in conjunction with CISA, NSC, NEC, and DOC, to produce or commission a study to determine differences between business-risk tolerance based on economics and societal and national-security-risk tolerance; then identify deltas and subsequently determine what cybersecurity practices should be incentivized to close these deltas.

The 2013 National Infrastructure Protection Plan stated that, "While individual entities are responsible for managing risk to their organization, partnerships improve understanding of threats, vulnerabilities, and consequences and how to manage them through the sharing of indicators and practices and the coordination of policies, response, and recovery activities." However, as international interactions increase in cyberspace, the level of cyberattacks on the public and private sectors have skyrocketed. For the private sector, the impact is staggering. Attacks result in reputation damage, lost revenue and opportunities, legal and social repercussions, as well as whatever lasting operational or infrastructure damage that was caused by the attack. The resulting impact on the economy, in terms of lost productivity and ransoms paid is massive. In fact, ransomware attackers are on pace for their second-biggest year ever, having extorted at least $449.1 million through June 2023, according to private sector company Chainalysis.[29]

Cyberattacks and the threat of cyberattacks against critical infrastructure entities (the majority of which are owned and operated by the private sector) are obviously particularly troubling, given their potential to disrupt and even upend everyday life. Although the private sector is well versed in mitigating risk from criminals, including cyber criminals, the extreme risk posed by nation-state actors and those affiliated with them is outsized. Specifically, critical infrastructure owners and operators are at risk due to the ability of nation-state actors to intimidate, project power, and pre-position in case of future (or current) hostilities. Therefore, the paradigm for public-private partnerships needs to evolve, and greater support is needed to help close the national security gap for private-sector cybersecurity investments.

The Cyber-Eco Model & Critical Infrastructure Outcomes[30] determine the overall investment required to implement and create a sustainable cybersecurity model to effectively address nation-state attacks while maintaining appropriate commercial service of critical infrastructure. There is a threshold level whereby investors

[29] Chainalysis. "Crypto Crime Mid-Year Update: Crime Down 65% Overall, But Ransomware Headed for Huge Year Thanks to Return of Big Game Hunting." July 12, 2023. https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/#:~:text=In%20fact%2C%20ransomware%20attackers%20are,trailing%20only%202021's%20%24939.9%20million.

[30] Briefing by Larry Clinton to the NSTAC Subcommittee.

are no longer willing or able to invest in additional security. The gap that exists between the funding needed for national security and the maximum investor threshold would need to be filled through some form of incentives. Based on presentations, NSTAC assessed that the key barrier that prohibits many organizations from adopting cybersecurity standards and best practices is that there are not enough resources or money.

To assume that critical infrastructure entities can and should remain wholly responsible for security not just at a commercial level but also when a nation-state attack occurs is a faulty assumption, so that funding gap needs to be filled. Most risk analysis, including at the macro level, uses sophisticated modeling with the inclusion of financial, environment, and geopolitical risk. Despite the vast majority of our national economy being digitally based, there is no current macro-economic model for cybersecurity. A comprehensive study on the differences between risk tolerance based on economic needs and risk tolerance based on national security needs can help inform policy makers and stakeholders to improve public-private partnerships and cybersecurity policy outcomes.

Part VII – Developing Metrics Literacy

Finding: Subjective measurements, combined with bad math, lead to ineffective decision-making; improved metrics literacy and a focus on leading versus lagging indicators can strengthen cybersecurity prioritization.

- **Priority Recommendation:** The president should task NIST with launching an effort, in partnership with stakeholders, to develop a mathematically defensible methodology for assessing cybersecurity measurements using existing cybersecurity survey data.

The NSTAC finds that the cybersecurity industry lacks "metrics literacy." Organizations attempting to measure security outcomes often use subjective, qualitative (i.e., words) measures but then perform mathematical operations on the results as if they were quantitative (i.e., numbers). Furthermore, the over reliance on qualitative metrics fails to give an organization insight into progress over time, fails to guide risk-based decision-making, and leads to choices that are at best suboptimal and at worst detrimental.

Quantitative metrics may similarly suffer from inherent limitations. They may only measure certain aspects of security and not cover others. For example, some presenters stated that their quantitative framework only covered 10-15 percent of the variance in breaches. Certain metrics, such as phishing click through rates, may be highly volatile and dependent on external factors rather than measure the underlying strength of controls. Quantitative metrics when absent context may result in the wrong conclusion. One presenter noted that in one of their organization's models, physical security-based controls had no impact on breaches. On further investigation it turned out that they simply did not have enough data in the control group. However, similar deep dives may not be conducted when a finding aligns with the 'assumed common knowledge' of the analyst. Thus, quantitative metrics must be combined with qualitative context tied to a decision and validated against external security outcomes to determine measurement coverage. Finally, it was found that little work had been done to assess the effectiveness of the measurement methods themselves.

Metrics Literacy

The CISA CPGs provide an easily understandable example of a qualitative measurement system, which can be used to illustrate problems with subjective measurements. The CGP worksheet asks participants to rate security controls in one of four ways:

1. Not Started
2. Scoped
3. In Progress
4. Implemented

These form an "ordinal" scale. Ordinal scales allow one to determine that one item is greater than or less than another, but they cannot say by how much. For example, it cannot be said that "scoped" is twice as good as "not started." Nor can it be said that two "scoped" controls are exactly as effective as one "implemented" control.

The working group observed that most organizations using such ordinal scales perform invalid mathematical operations such as multiplication and division on them. For example, an organization might assign the four CPG categories numbers 1-4 and average the ratings. This leads to nonsensical results such as stating that an organization's security posture is "2.37." If level 2 means "scoped," what does it mean for a security program's maturity to be "scoped plus .37?" How can a security leader decide where to spend limited budget dollars with no way to determine whether bringing one control from a 2 to a 3 has more impact than bringing another control from 1 to 2?

As a follow on, it should be noted that ordinal scales such as these suffer from "range compression." Range compression occurs when a spectrum of values is compressed into a small number of buckets. For example, imagine that an organization rates its risks as "low," "medium," or "high." Further suppose that it defines a low risk as anything less than $100,000, a medium risk as $100,000 to $1m, and a high risk as anything higher than $1m. Using such a system, an organization cannot distinguish between a $2m risk and a $2bn risk because both are "high." Qualitative control maturity scales suffer from the same problem. In the case of the CPGs, an organization that improves an "implemented" control sees no change in measurement even if the control becomes much more effective. Furthermore, range compression precludes organizations from being able to measure incremental progress during implementation. A control might remain "in progress" for months even though a great deal of work is being performed because it has not crossed the finish line to "implemented."

Over Reliance on Qualitative Measurements

The working group finds that invalid scoring systems created from ordinal measurements, combined with the fidelity lost due to range compression, lead to poor decision-making. Because such ordinal scales provide no insight into the amount of risk reduced by implementing one control over another, organizations make decisions based on gut instinct, improving imaginary scores, tackling whatever is cheapest or easiest, or simply looking at other organizations within the same sector and copying them. To make informed, risk-based decisions, security

leaders must be able to understand the magnitude of risk reduced by progress in a category, and qualitative measurements do not provide that.

Limitations of Quantitative Measurements

Security, like happiness, is a subjective property of a system. Quantitatively measuring security thus runs the risk of only measuring certain aspects while underreporting others. For example, it is easier to measure the number of open vulnerabilities and harder to measure security culture. Furthermore, some metrics may be based on more than just the strength of the underlying controls and instead be influenced by external factors.

It is critical to consider how quantitative metrics are designed in order for them to be effective at driving security investments. First, quantitative measurements should be tied to a security outcome and be the driver of a distinct investment decision. These individual or combination of measurements should be validated by examining their ability to explain the variance in the security outcomes to ensure both that they are the correct metrics and that they are accurate metrics.

Assessing the Effectiveness of Measurements

The working group finds that insufficient work has been done to assess the effectiveness of cyber security measurements. Do current measurement strategies actually inform decisions that lead to fewer compromises?

The NSTAC makes the following additional recommendations:

- **Recommendation:** The president should task NIST, in collaboration with CISA to partner with the private sector to develop a methodology and mechanisms to assess the performance of measurement methods that can be leveraged by the new Department of Commerce-led governmentwide Measurement Center of Excellence.

- **Recommendation:** The president should task NIST, in collaboration with CISA, to develop material to educate and encourage organizations to adopt more quantitative risk management strategies.

Part VIII – Partnering with the Private Sector to Assess Adoption and Effectiveness

Finding: Private firms may hold data that can serve as a proxy to measure best-practice adoption.

- **Priority Recommendation:** The president should task the proposed Cybersecurity Measurement Center of Excellence within DOC, in collaboration with appropriate federal agencies and state governments, to study whether firms such as cyber insurance companies have information/data that could be shared voluntarily with the government in an anonymized fashion that could help assess the state of best-practice adoption and the impact of cyber insurance on best-practice adoption. The study should establish and publish a broad set of metrics, which may provide guidance for other companies to follow. In addition to assessing the current state of practice, such data may also provide a tool for measuring the effectiveness of future policies and programs.

Several types of firms may be able to provide aggregate data about the use of cybersecurity standards and best practices: cyber-insurance firms, cybersecurity service providers, and certification bodies. Through the course of business, these firms become familiar with the cybersecurity readiness of their client base.

Aggregate data from such firms may be used to approximate the current rate of implementation of cybersecurity standards and best practices, as well as changes over time. Such data may also provide insights into the effectiveness of future policies and programs.

The cyber-insurance industry allows eligible companies to acquire coverage for cybersecurity risk. Companies are underwritten based on the completion of a cybersecurity evaluation that is conducted by a prospective insurer. Underwriting is a complex process, and evaluation criteria can vary significantly by industry and company risk profile. The rigor that is applied to evaluations of companies can vary based on company size and coverage magnitude: a small company may only be subject to answering a limited number of questions, while a larger company may be subject to significantly more scrutiny. Cyber insurers work to diversify their risk portfolio across an acceptable set of insured companies. They then further aggregate this risk through the cyber-reinsurance industry. The cyber-reinsurance industry introduces a standardizing dynamic: reinsurers play a role in establishing the criteria for policy coverage allowances throughout the cyber-insurance marketplace. This has the effect of creating effective standards for coverage, policies, and cyber-insurance measurements.

Cybersecurity service providers may offer a full-range service to manage the security of an enterprise, or they may provide specialized tools that a business can incorporate into their risk management system (e.g., tools to detect and respond to vulnerabilities and incidents). The former in particular (and the size and demographics of their client base) can provide information about their practices and the standards with which they are aligned.

Certification bodies, auditors for certification schemes such as SOC 2 or ISO/IEC 27001, are another source of information regarding qualified audits, the number and types of firms that have been certified, and common challenges that their clients face.

The American Institute of Certified Public Accountants (AICPA) established the widely recognized System and Organization Controls (SOC) suite of certifications for service organizations. SOC certifications must be performed by an independent AICPA-licensed CPA. AICPA provides a searchable database of AICPA firms.[31]

The International Accreditation Forum (IAF) provides a searchable database of certification bodies by economy and by a select set of ISO management-system standards.[32]

Many insurers have developed proprietary scoring mechanisms and take pride in their risk-oriented datasets from their own perspectives. Performant cyber insurers have each created their own direct or indirect measurement criteria for measuring cyber risk. Secondary markets have also been established around this measurement ecosystem, such as companies that work to help companies navigate the underwriting processes

[31] American Institute of Certified Public Accountants. “CPA License Verification - Find a CPA.” https://us.aicpa.org/forthepublic/findacpa

[32] International Accreditation Forum. “IAF Certification Bodies.” https://www.iafcertsearch.org/search/certification-bodies

while helping companies decrease their risk exposure. A key metric has emerged within the domain of actively managing company cyber insurance versus risk, called the Loss Exceedance Curve. Loss Exceedance represents the amount of financial exposure a company is willing to take on relative to their current coverage.

The economics within a free market have resulted in the organic emergence of systems that adapt to market dynamics. There are some challenges that have also emerged:

a. The cyber insurance industry has a total capital capacity which may not fully cover the entirety of its exposure in the event of major changes to threats (such as the onset of ransomware attacks in 2020-22). This has principally resulted in the adaptation of premiums and rigor required for cyber-insurance coverage (a free market response), but there can be a latency with insurance premiums and evaluation-measurement phases that are subject to evaluator latency that cannot respond as rapidly as the emergence of these high-impact categorical cybersecurity threats.

b. Exclusions in the cyber-insurance industry may result in lack of coverage and unintended consequences for national security. The reinsurance industry has established de facto standards for cyber insurers that have resulted in these categorical exclusions. While such exclusions can be prudent given the market size, these exclusions may not be in the best interests of critical infrastructure protections and national security interests. They can result in ineligibility of system application due to company interests in minimizing Loss Exceedance.

The NSTAC makes the following additional recommendations:

- **Recommendation:** The president should task the Department of Treasury to perform a study to provide a recommendation on the expected effects of a cyber-insurance backstop relative to insurance industry capital responsiveness with the aim of seeking to close the gap between insurance offered by the market and the needs of national security and emergency preparedness.

- **Recommendation:** The president should task ONCD, in partnership with CISA and the Office of the Secretary of Defense to evaluate the effects of categorical insurance exclusions and respective impacts to critical infrastructure and national security and emergency preparedness risk exposure.

Part IX – Addressing Workforce Shortages and Talent Gaps

Finding: Lack of qualified personnel, as well as a lack of resources to recruit and retain qualified personnel, is consistently cited as both a barrier to adoption of best practices and a barrier to effective cybersecurity measurement.

- **Priority Recommendation:** The president should direct ONCD, in coordination with DOD, CISA, NIST, NSF, and other government stakeholders, to establish virtual national cyber academies to provide free training in exchange for service. Outreach for these programs should have a strong focus on enhancing diversity in cybersecurity professions. Placement roles could be either within government cyber functions or with a commercial enterprise that is part of a critical infrastructure coalition or partnership, prioritizing smaller

companies that may lack cybersecurity resources. Cybersecurity courses would be the focus of education with partner colleges and universities providing supplemental coursework.

There are hundreds of thousands of vacant cyber jobs due to a significant shortage of skilled cyber professionals. The shortage is consistently cited by briefers as both a barrier to adoption of best practices and a barrier to effective measurement. The increasing cybersecurity threats and demands are a major challenge for government and industry workforces. In addition to the consistent and expanding attack scenarios requiring constant risk-management responsibilities, emerging technologies and increased political attention are requiring new approaches to our cyber-response strategy.

According to the National Skills Coalition's 2023 Digital Divide Report, 92 percent of jobs across industries in the United States require at least some digital skills.[33] In 2022, the United States had close to 750,000 unfilled positions. Mission Square Research Institute notes the state and local government job opening rates are at the highest level in 20 years. Currently, the demand exceeds our supply impacting our ability to source new talent and battle cyber burnout.

Key challenges to building our cyber workforce and education system: hundreds of thousands of vacant cybersecurity jobs; an insufficiently diverse workforce to fill those jobs; and barriers to accessing cyber education and training.

Multiple drivers will shape America's cyber-workforce needs, but meeting demand for skilled cybersecurity workers in critical-infrastructure sectors is an urgent national concern. The National Cyber Workforce and Education Strategy is intended to meet the President's National Cybersecurity Strategy Mandate.[34] Focusing on efforts to engage women, minorities, and other underrepresented groups like disabled workers in the cyber workforce can help access potential pools of labor to fill existing gaps. Workforce initiatives can also look to service members exiting the U.S. armed forces, many of whom have some form of cyber training or certification. Private-sector organizations can follow this example of targeting community colleges, trade schools, and colleges serving traditionally underserved populations as a source of cyber talent by offering scholarships and collaborating with learning institutions to build training and certification courses to fit industry needs.

The United States and its partners must navigate this decisive decade to build a defensible, resilient, values-aligned digital environment that furthers security, economic prosperity, and technological innovation.

Call to Action: All stakeholders, public and private partners, and academia can contribute to the implementation of this National Cyber Workforce and Education Strategy. Cyber skills must be drastically scaled up to deliver this future, keep America secure, and ignite the next generation of American innovation.

---

[33] National Skill Coalition. "Closing the Digital Skill Divide." February 6, 2023. https://nationalskillscoalition.org/resource/publications/closing-the-digital-skill-divide/

[34] The White House. "National Cyber Workforce and Education Strategy." July 31, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

The NSTAC makes the following additional recommendations:

- **Recommendation:** The president should task NIST with leading an effort, in coordination with Department of Education, DOL, and CISA, to promote best practices for people-based cyber-resilience training based on the NICE Framework.

- **Recommendation:** The president should direct OPM, in partnership with DOL, to develop guidance for public and private sector organizations to utilize competency-based hiring to fill workforce gaps.

- **Recommendation:** The president should task ONCD with developing a strategy to mobilize cybersecurity experts, including retired computer-security professionals, to support a "Cyber Corps" where computer-security experts can volunteer to assist small businesses that need cybersecurity expertise but would have difficulty investing in a full-time employee or managed service.

Part X – Promoting Secure Software Development Practices

Finding: Phased approaches to secure software-development requirements can strengthen outcomes.

Priority Recommendation: The president should direct CISA to seek maturity-model guidance or standards from the private sector and, in consultation with the private sector, to develop reasonable compliance timeframes for completing the OMB/CISA Secure Software Self-Attestation Common Form (SSSCF). Attestation alone may provide some insight for federal agencies, but there is significant risk that it may prevent adoption of innovative or mission-critical software products and services. Maturity modeling can bring added granularity and understanding of risks associated with the security posture of a software product that can enable end-users to make more informed risk-based decisions.

Numerous ongoing U.S. government efforts exist to incentivize and inform secure software development. Efforts include the NIST Secure Software Development Framework (SSDF), Software Bill of Materials (SBOM), CISA's Secure-by-Design/Secure-by-Default initiative, the SSSCF, and others. Each of these elements can play an important role in improving the security of the software-development supply chain, but these efforts could benefit from a more cohesive approach in using them together to drive change more consistently.

These efforts have been created to:

- Ensure end users (both consumers and enterprises) have adequate information about the security features and potential weaknesses (current and future) in software products that could negatively impact the software's ability to function as expected and/or prevent the unauthorized exposure of sensitive information (PII, PHI, IP, company proprietary, etc.).

- Inform software developers on the best practices for ensuring their software does not ship with known vulnerabilities or weak configurations that create risk for users of that software.

However, it is well understood that the U.S. government cannot, by itself, cause the widespread change needed to ensure secure software development practices and elevate the overall security of the software supply chain globally.

To date, regulatory efforts have proven ineffective, despite some progress being made in certain sectors, such as with FDA guidance regarding medical devices. As such, additional regulation is unlikely to produce results unless it can be informed by sufficient study and understanding regarding the nature of the challenges.

One such challenge is the prevalent use of open-source software in a majority of software products sold to consumers, enterprises, and governments. The benefits of open-source software have been well understood for decades, and open-source software has enabled, in large part, the rapid evolution of the internet and countless supporting and adjacent technologies. More recently, the risks associated with the widespread use of open-source software have become more apparent. This has driven significant interest in the development of SBOM and the other initiatives noted in this report.

The true scope of the risk introduced by open-source software remains elusive even as awareness of the problem continues to grow.

NSTAC makes the following additional recommendations:

- **Recommendation:** The president should task NIST with seeking private-sector-developed maturity-model guidance or standards that can be applied to the SSDF. If such guidance does not exist or is not under development, NIST should develop such guidance with private sector input. Such guidance or standards should be used to account for inclusion of various practices and processes in the SSDF guidance and avoidance of common software-development practices that are known to produce weaknesses. This guidance should contemplate that companies attesting compliance with the SSSCF in order to qualify for procurement opportunities are likely—at least for the time being—to identify gaps, which will require clearly articulated plans of action and milestones (POA&Ms). The transparent communication from vendors to customers of both current SSSCF capabilities as well as plans to close gaps via POA&Ms should reasonably drive clearer market signals for adoption of secure software-development practices.

- **Recommendation:** The president should task NIST, in coordination with CISA, other relevant federal agencies, and the private sector, to create a Grand Challenge focused on the impacts of using open-source software and how the federal government can further incentivize the creation of resources designed to improve the quality and security of open-source software without impacting innovation.

Part XI – Leveraging Advanced Technologies to Improve Cyber Defenses

Finding: Public and private sector organizations should be encouraged to leverage effective technologies that level the playing field against attackers or give defenders an advantage.

- **Priority Recommendation:** The president should task ONCD, in coordination with CISA, NIST, and DOE, to create a Cybersecurity Grand Challenge for organizations to leverage next-generation artificial

intelligence/machine learning (AI/ML) capabilities, including large language models, to effectively drive adoption and use of cybersecurity best practices and enable more efficient measurement of their use. The long-term vision for this work should include assessing whether and to what extent the use of AI, conducted under human supervision, might either help to bridge the talent gap in AI by democratizing access to previously complex security technologies and capabilities and/or enable certain actions to be taken without direct human intervention.

Advanced technologies, such as AI/ML, can improve cybersecurity programs in key measurable ways. AI/ML-enabled 'copilots' can assist information security professionals' decision-making as they evaluate their organizational security posture and how corporate cybersecurity policies and established best practices are being effectively implemented. AI-enabled security tools also can more effectively automate cyber-threat prevention, helping triage large data sets that cannot otherwise be reviewed by humans fast enough to detect, protect, and respond to modern day attackers.

Some examples of advanced technology capabilities, many of which are commercially available today, include:

1. Improved security-development practices: AI/ML systems that write and debug code can do so faster and more comprehensively on large code sets than human developers. In turn, human developers learn from the security defects that AI/ML systems identify and fix so they can write better code with fewer defects.

2. Early threat detection and improved monitoring and alerting: AI/ML systems can quickly examine very large data sets such as log files generated by busy network firewalls, web-application firewalls, intrusion-detection systems, intrusion-protection systems, domain-name system servers, and other sources of rich security data. AI/ML systems can perform such reviews for anomalous activity at greater speed and scale, giving defenders a better chance to detect and stop attackers in the early stages of their attacks, even if the threat vector or attack technique was previously unknown.

3. Improved incident-response capabilities: AI/ML systems combined with security technologies such as extended detection and response and security orchestration, automation, and response can help security teams increase the speed and efficiency of their responses to security incidents thus potentially reducing the blast radius of attacks, reducing dwell time of attackers in their IT environments, and reducing associated costs of recovery.

4. Ease adoption of cybersecurity best practices: AI/ML systems may ease the ability of workers—even those without training, certifications, or experience—to interact with security technologies using natural-language capabilities in ways that improve baseline-security outcomes. For example, AI systems leveraging chatbots may enable managers to provision access to systems with appropriate role-based access controls for new hires—or to terminate access upon separation by an employee—using natural-language queries without the need to interact with complex, technical rule-management systems.

5. AI-enabled vulnerability management and remediation: Many organizations struggle to understand and manage their internet-facing attack surfaces. AI-powered tools can help organizations continuously map

the vast public-facing internet to discover an organization's exposed assets, vulnerabilities, and misconfigurations through the eyes of the adversary, empowering human analysts to remediate in a prioritized manner accordingly.

AI/ML systems can add value to existing cybersecurity investments in scenarios where there are very large data sets that cannot be reviewed by humans fast enough to detect, protect, and respond to modern day attackers.

The 2018 *NSTAC Report to the President on a Cybersecurity Moonshot* report included recommendations for assessing opportunities to leverage AI/ML for cybersecurity purposes. In addition, the report recommended launching Cybersecurity Grand Challenges, where an "accelerated whole-of-nation focus could produce demonstrable progress over a three to five-year time horizon."[35] "These recommendations could be combined to develop a Cybersecurity Grand Challenge to leverage AI and ML to identify stronger mechanisms to measure the effectiveness of cybersecurity best-practice adoption.

The NSTAC notes that National Cybersecurity Challenges, with specific reference to the importance of emerging technologies including AI, became law with the president's signature of the Mac Thornberry National Defense Authorization Act for Fiscal Year 2021. The law directs the Secretary of Commerce, in consultation with the White House, Secretary of Homeland Security, and other agencies to establish national cybersecurity challenges to accelerate innovation toward the achievement of strategically transformative cybersecurity objectives. The NSTAC is unaware of any progress toward implementation of these challenges.

The NSTAC makes the following additional recommendation:

- **Recommendation:** The president should direct CISA to identify highly effective security use cases for AI/ML systems and publish automation templates and accompanying documentation to enable organizations to rapidly deploy such systems using cloud infrastructures. This will enable small and medium-sized organizations without dedicated cybersecurity or automation teams to benefit from AI/ML and improve their cybersecurity capabilities. It will also reduce costs for larger, more mature organizations that would otherwise have to develop their own similar capabilities, while improving their cybersecurity posture.

Part XII – Measuring and Tracking Progress Toward a Healthy Cybersecurity Culture

Finding: A healthy security workplace culture is a leading indicator of strong cybersecurity. It encompasses the mindset, behavior, and practices of an organization toward security, and it is a crucial aspect of building long-term resilience against cyber threats.

- **Priority Recommendation:** The president should task the Computer Science and Telecommunications Board of the National Academy of Sciences to conduct a study on how best to measure and track

[35] National Security Telecommunications Advisory Committee. "NSTAC Report to the President on a Cybersecurity Moonshot." November 14, 2018. https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf

progress toward healthy security culture, which is a leading indicator of strong cybersecurity and cyber resilience.

Organizations that have strong cybersecurity cultures typically have higher levels of awareness, readiness, and resilience in the face of constantly evolving cyber risks. Organizations that are successful at integrating cybersecurity into their corporate cultures are in a better position to protect, detect, and respond to modern-day threats. Therefore, cultivating strong cybersecurity cultures among organizations in the private and public sectors should be encouraged and incentivized.

Additionally, given the shortage of trained cybersecurity workers in today's workforce, both public and private-sector organizations struggle to fill open roles. Having a strong workplace culture helps to attract, develop, and retain cybersecurity talent by providing a supportive working environment. Effective governance can help create a strong enterprise-wide cybersecurity culture, which informs and influences how people work and protect their organizations from cyber threats.

Organizations have multiple levers to develop strong cybersecurity cultures, including:

- Cultivate a cybersecurity culture.
- Create a clearly stated vision that is self-reinforcing within organizations.
- Prioritize having a diverse and inclusive workplace.
- Include cybersecurity training and awareness programs to educate workers about cyber threats, how to identify them, and expected behaviors and outcomes.
- Reward behaviors that are desirable and consistently show that there are consequences for behaviors that are undesirable.

Despite significant investments being made to improve cyber defenses, a healthy security culture is frequently deprioritized or left behind in the pursuit of improving direct cyber defenses or lagging indicators of cyber resilience.

According to a report by the World Economic Forum, a diverse and inclusive workplace is a key driver of resilience and recovery, noting that it plays a critical role in the high performance of businesses, economies, and societies globally.[36]

There is ample evidence that diversity and inclusivity in the workplace are essential for developing effective solutions, addressing the needs and challenges of different groups, improving retention rates and job satisfaction, and fulfilling the moral imperative of protecting all individuals. In the context of some of the current

[36] United Nations. "Diverse, inclusive workplace: 'Key driver of resilience and recovery'." April 6, 2020. https://news.un.org/en/story/2022/04/1115672

challenges in cybersecurity, a diverse and inclusive workforce can help solve the acute talent shortage in the industry.[37] Here are some other reasons why diversity and inclusion are important in cybersecurity:

1. **Different perspectives:** A diverse workforce brings a variety of perspectives and experiences to the table, which can help identify and address security risks that may have been overlooked otherwise. In addition, a diverse cybersecurity workforce can help organizations better understand and analyze human behavior, motivations, and intent, which are all necessary elements in identifying, combating, and mitigating cyber-attacks.[38] For example, some researchers have proposed six specific diverse traits that could be used to select personnel within the cyber domain (systemic thinkers, team players, technical and social skills, civic duty, continued learning, and communication).[39] Further, research identifies neurodiversity as a competitive advantage that should be leveraged by the cybersecurity field.[40]

2. **Increased Innovation:** A diverse team can foster innovation by encouraging creativity and out-of-the-box thinking. A diverse cybersecurity team can help organizations better protect their digital and physical infrastructure by providing a range of perspectives and approaches to cybersecurity challenges.[41]

3. **Better problem-solving:** A diverse team can approach problems from different angles, leading to more effective solutions. Diverse perspectives can lead to better problem-solving in cybersecurity by bringing in a variety of viewpoints and experiences that can help identify and address security risks that may have been overlooked otherwise.[42]

4. **Improved retention rates:** A diverse and inclusive work environment can improve employee retention rates and job satisfaction.[43] According to a 2023 cybersecurity job statistics report, 60 percent of organizations surveyed in 2021 reported difficulty retaining skilled cybersecurity employees. Employees' perception of their company's diversity, equity, and inclusion efforts has a significant impact on their job satisfaction.[44]

---

[37] World Economic Forum. "Why Cybersecurity Needs a More Diverse and Inclusive Workforce." October 26, 2021. https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/

[38] Microsoft. "Why diversity is important for a strong cybersecurity team." September 9, 2021. https://www.microsoft.com/en-us/security/blog/2021/09/09/why-diversity-is-important-for-a-strong-cybersecurity-team/

[39] Dawson, J.; R. Thomson; "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," *Frontiers in Psychology,* 2018

[40] Curry, S, Forbes. "Neurodiversity: A Competitive Advantage in Cybersecurity." May 13, 2019. https://www.forbes.com/sites/samcurry/2019/05/13/neurodiversity-a-competitive-advantage-in-cybersecurity/?sh=3495ac406265

[41] World Economic Forum. "Why Cybersecurity Needs a More Diverse and Inclusive Workforce." October 26, 2021. https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/

[42] Gitnux. "Cybersecurity Diversity Statistics." December 16, 2023. https://blog.gitnux.com/cybersecurity-diversity-statistics/

[43] Forbes. "Prioritize Diversity In Your Cybersecurity Teams For Better Business Results." December 14, 2021. https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/14/prioritize-diversity-in-your-cybersecurity-teams-for-better-business-results/?sh=1d0425cd3d14

[44] Momentive AI. "Key to Retaining Employees." https://www.momentive.ai/en/blog/dei-key-to-retaining-employees/

5. **Minimized skills gap:** The demand for cybersecurity professionals is rising globally as cyberattacks are increasing in scale and severity. Attracting diverse candidates can help improve the acute talent shortage in cybersecurity. An abundance of research exists on the reasons behind the large and rapidly expanding gap in cybersecurity personnel and the vacant positions left unfilled due to the lack of qualified candidates. The shortage of cybersecurity personnel is not isolated to any one country or region, and the disparity among women, minorities, and neurodiversity is a concern across the globe.[45]

Measuring and Tracking Progress Toward a Healthy Security Culture

Company executives and boards currently manage cybersecurity risk through Enterprise Risk Management (ERM) frameworks. In recent years, there has been increased focus by corporate stakeholders on Environmental, Social, and Governance (ESG). ESG reporting is in its early stages and is evolving year over year. As part of the study, ESG was suggested as an avenue to investigate how it could be used to improve cybersecurity governance. ERM frameworks are robust and address cyber risks alongside other organizational risks. It will be important to understand the evolution of ESG reporting and its relationship to ERM governance.

While commonly used reporting frameworks include security-related disclosures (such as numbers of data breaches or system average interruption frequency), they currently do not include reporting on elements specific to social aspects of healthy security culture. For this reason, further study is needed on improving cybersecurity culture as it may serve as a prominent predictor of cyber resilience.

Conclusion

There are strong market incentives for critical infrastructure and other private-sector organizations to adopt cybersecurity best practices. Competitive differentiation, reputational protection, and customer demands are all strong economic incentives for deploying effective cybersecurity practices. Indeed, at an aggregate level, private-sector organizations have significantly increased investments in cybersecurity people, processes, and technologies over the last 20-plus years. However, despite these increased investments, cyber-attacks against critical-infrastructure systems continue to occur at an alarming pace. Due to the increasingly connected nature of our critical-infrastructure systems, these cyber-attacks may have significant downstream effects on national security, economic security, and emergency preparedness.

Private-sector entities generally make cybersecurity investment decisions on a range of economic, regulatory, and other factors. They are usually willing to accept a certain amount of risk based on these calculations. Governments, including the U.S. government, have additional equities, such as national security, safety and health, and aggregate economic security, which inform their cybersecurity priorities. As a result, there can be a gap between the optimal cybersecurity investments that critical infrastructure and other private-sector

[45] ISACA. "Cybersecurity Workforce Diversity—Including Cultures, Personalities and Neurodiversity." October 12, 2021. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/cybersecurity-workforce-diversity-including-cultures-personalities-and-neurodiversity

organizations will make based on economic factors, and the investments that governments believe are needed to adequately ensure national security and other societal needs.

As a result, there is a significant need for the U.S. government to provide incentives to motivate private-sector actors to adopt cybersecurity best practices at a level needed to close the economics-based and national security-based cybersecurity gap. Further, there is a need for the U.S. government to promote the effective use of cybersecurity measurements and metrics to help organizations more fully understand these adoption levels.

Different types of incentives will be required to motivate different types of organizations based on their cybersecurity maturity levels and other factors. For instance, motivating incentives, such as tax deductions and liability protection, will help strengthen adoption rates among more mature organizations and those with resources to invest in cybersecurity. Enabling incentives, such as free cybersecurity services and comprehensive cybersecurity guidance will help less mature entities that lack resources to invest in cybersecurity. Regulatory alignment around best practices, such as the NIST CSF 2.0 and the CISA CPGs, will significantly ease compliance burdens for both more mature and less mature organizations.

To close the national security gap more effectively, the government and its private-sector partners must have a shared understanding of the cybersecurity environment. This understanding depends on effective measurements and metrics, and these measurements and metrics depend on effective utilization of data. The establishment of a Cybersecurity Data Center of Excellence can help leverage existing cybersecurity data and inform future private-sector data-normalization efforts. Government can also work with the private sector to drive stronger cybersecurity metrics literacy. And government can partner with private-sector and nonprofit entities to assess how they can utilize the data they hold to assess cybersecurity best-practice adoption.

The adoption of cybersecurity best practices depends on multiple additional factors as well. These include implementing effective workforce strategies and understanding the role advanced technologies such as AI and ML can play to improve cybersecurity outcomes. And, critically, adopting stronger organizational cybersecurity culture will be required to underpin each of these advancements in a sustainable way.

The successful implementation of the recommendations included in this report will help the country achieve a stronger cybersecurity posture and reduce risks to national security. The NSTAC stands ready to help support the president and administration to dramatically improve the adoption of cybersecurity best practices.

Appendix A. Table of Cybersecurity Frameworks and Requirements

Framework	Requirement					
	Access Review Freq.	**Incident Reporting SLA**	**Vulnerability Scanning Freq.**	**Penetration Testing Freq.**	**Log Preservation**	**Encryption Strength**
ISO 27002	Access reviews be conducted **at least annually** or more frequently depending on the nature of the information being accessed	**No specific incident reporting timelines** – establish incident mgmt. process that include clear procedures for reporting, assessing, and responding to security incidents	ISO 27002 requires organizations to **perform regular vulnerability scanning** on internal and external networks, web applications, and other information systems, but leaves the specific frequency of the vulnerability scanning up to the organization's discretion based on a comprehensive risk assessment.	No specific frequency requirement for pen testing – ISO 27002 recommends pen testing be **conducted regularly** and should be risk based	Does not establish specific requirements for log retention periods. Organizations are required to implement a process for the collection, preservation and storage of log data related to information security events.	ISO 27002 recommends the use of strong encryption algorithms to protect confidential and sensitive information and specifies that the **appropriate encryption strength** to be used should **depend on the confidentiality classification** attributed to the data
NIST 800-53	Access reviews should be conducted **at least annually** or more frequently depending on the nature of the information being accessed	No specific incident reporting timelines – establish incident mgmt. process	The **minimum frequency for vulnerability scanning is annually,** but organizations may choose to scan more frequently for high-risk systems or when regulatory or contractual requirements dictate a higher frequency.	The **minimum frequency for high-risk systems is annually**, but organizations may choose to conduct testing more frequently for high-risk systems or when regulatory or contractual requirements dictate a higher frequency.	Does not establish specific requirements for log retention periods. Requires that logs generated by information systems be retained for a specific period based on the informational value of the log data.	Use **AES with minimum key lengths of 128 bits for data at rest and 192 bits for data in transit**, while also incorporating other cryptographic algorithms for specific purposes.
DFARS 7012	Contractors are required to review and update user access permissions **no less than annually**	Any cybersecurity incidents involving CUI must be reported to the DoD within **72 hours** of discovery.	DFARS 7012 requires vulnerability scanning of covered contractor information systems **at least quarterly. Additionally, if any significant change occurs in the system being scanned,**	The frequency of penetration testing required by DFARS 7012 should be **based on a comprehensive risk management strategy** that considers the size and complexity of the information	Contractors **must preserve audit log information for a minimum of six years** from the date of creation, protect it from unauthorized access, and conduct regular reviews to ensure	Encryption must be based on approved **FIPS 140-2 compliant algorithms** with **AES 128-bit minimum and 256-bit for top-level protection.**

			such as the addition of new software or infrastructure, a scan must be conducted prior to or within 30 days of the change.	system, the types of data processed, and the level of risk associated with the system.	compliance with the mandate.	
NIST 800-171	Conduct **periodic access reviews** to ensure that only authorized users and processes have access to CUI.	No specific incident reporting timelines - establish incident mgmt. process	NIST 800-171 requires that vulnerability scans be conducted **at least quarterly** on all systems within the scope of the information system and their associated interfaces. In addition, **any significant changes to the system**, including hardware or software changes, network configurations, or updates, **should trigger a new vulnerability scan.**	Does not provide a specific frequency for conducting penetration testing, but it recommends that organizations establish and maintain an ongoing security assessment program.	Does not establish specific requirements for log retention periods. However, it does recommend that organizations establish retention periods for log data based on legal, regulatory, and business requirements.	For data at rest, the encryption solution must use an approved algorithm selected from the NIST SP 800-131A Rev. 2 ITL Bulletin.
						The encryption strength must be a **minimum of 128 bits if using symmetric key** algorithms**, or equivalent for asymmetric key algorithms.**
PCI DSS 4.0	Implement a process for **regular access reviews** and to identify unauthorized or inappropriate access.	No specific incident reporting timelines - establish incident mgmt. process	PCI DSS 4.0 also requires organizations to **conduct quarterly vulnerability scans** to identify potential security vulnerabilities.	Organizations **must perform penetration testing on an annual basis** or after significant changes to their environment, such as changes to system components, processes, or technology.	Organization must retain audit trail history for a **minimum of one year,** with at least the most recent three months' logs available for immediate analysis, to support PCI DSS and investigations into security incidents.	For data at rest, PCI DSS 4.0 requires the use of strong and secure encryption algorithms, with **at least 128-bit encryption strength for symmetric key algorithms**, or at least **2048-bit encryption strength for asymmetric** key algorithms.
						For data in transit, requires the use of cryptographic protocols that meet industry best practices. **At least 128-bit encryption strength for symmetric key**

						algorithms, or at least **2048-bit encryption strength for asymmetric** key algorithms.
SEC incident reporting rule	Implement a process for **regular access reviews** and assessment of access controls to ensure that only authorized users have access to customer records and information.	Companies are required to report it in their public filings within a **timely manner**, which is generally considered to be a **few days up to a week after the event.** The SEC does not specify a specific incident reporting timeline for material cybersecurity incidents.	SEC requires organizations to **perform regular vulnerability scans** to identify and address any security weaknesses in their systems.	The SEC incident reporting rule does not provide a specific frequency requirement for penetration testing, but organizations should develop a process for assessing the materiality of cybersecurity incidents or risks and conduct regular vulnerability assessments and penetration testing	The SEC Incident Reporting Rule mandates broker-dealers to retain all written, electronic, or oral communications related to security incidents, including logs related to cyber incidents, **for a period of at least six years.**	The rule **does not specify** any particular encryption strength requirements.

Appendix B. Membership and Participants

Table 1: Subcommittee Leadership

Name	Organization	Role
Mr. Matt Desch	Iridium Communications Inc.	Subcommittee Co-Chair
Mr. Jack Huffard	Tenable, Inc.	Subcommittee Co-Chair
Ms. Kim Keever	Cox Communications	Subcommittee Co-Chair
Mr. Jamie Brown	Tenable, Inc.	Working Group Co-Lead
Lt Gen John Campbell, USAF, Ret.	Iridium Communications Inc.	Working Group Co-Lead
Mr. Matt Carothers	Cox Communications	Working Group Co-Lead
Mr. William Conner	Iridium Communications Inc.	Working Group Co-Lead
Mr. Chris Day	Tenable, Inc.	Working Group Co-Lead

Table 2: Subcommittee Membership

Name	Organization
Mr. Chris Anderson	Lumen Technologies, Inc.
Mr. Matthew Areno	Intel Corp.
Mr. John Banghart	Venable, LLP
Ms. Anne Borozan	Microsoft Corp.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Marty Edwards	Tenable, Inc.
Mr. Victor Einfeldt	Iridium Communications Inc.
Mr. Vaibhav Garg	Comcast Corp.
Mr. Matt Grote	Cybersecurity Division (CSD), Cybersecurity and Infrastructure Security Agency (CISA)
Mr. Joel Johnson	Lockheed Martin
Mr. Russell Kendall	Tenable, Inc.

Name	Organization
Mr. Kent Landfield	Trellix
Mr. Robert Lord	CSD, CISA
Mr. Joel Max	Siemens USA
Mr. Sean Morgan	Palo Alto Networks, Inc
Ms. Helen Negre	Siemens USA
Ms. Elaine Newton	Oracle Corp.
Ms. Ista Pinon	Cisco Systems
Mr. Alex Pinto	Verizon Business
Mr. Tom Quillin	Intel Corp.
Ms. Jennifer Raiford	Unisys Corp.
Mr. Tim Rains	T-Mobile
Mr. Kevin Reifsteck	Microsoft Corp.
Mr. Nick Saunders	Viasat, Inc.
Ms. Manjula Sriram	Iridium Communications Inc.
Ms. Stephanie Travers	Lumen Technologies, Inc.
Mr. Eric Wenger	Cisco Systems

Table 3: Briefers, Subject-Matter Experts

Name	Organization
Ms. Vera Adams	Transportation Security Administration (TSA), U.S. Department of Homeland Security
Mr. Peter Altabef	Unisys
Mr. Bret Arsenault	Microsoft
Mr. Matt Carothers	Cox Communications
Ms. Julie Chua	U.S. Department of Health and Human Services (HHS)

Name	Organization
Mr. Larry Clinton	Internet Security Alliance
Mr. Peter Colombo	CSD, CISA
Mr. Dan Daly	TSA
Mr. Burzin Daruwala	Intel
Mr. Erik Decker	Intermountain Healthcare
Mr. Kevin Frederick	TSA
Mr. Vaibhav Garg	Comcast Corp.
Mr. Harlan Geer	TSA
Mr. Scott Gorton	TSA
Mr. Matt Grote	CSD, CISA
Mr. James Hadley	Immersive Labs
Mr. Peter Haigh	United Kingdom, National Cyber Security Centre (NCSC)
Mr. Davis Hake	Resilience Insurance
Ms. Melissa Hathaway	Hathaway Global Strategies, LLC
Ms. Lauren Boas Hayes	CSD, CISA
Mr. Mitch Herckis	Office of Management and Budget (OMB)
Mr. Douglas Hubbard	Hubbard Decision Research
Mr. Bob Huber	Tenable, Inc.
Mr. Bryan Hurd	Aon Cyber Solutions (Stroz Friedberg)
Ms. Diana Kelley	Protect AI
Mr. Steve Kelly	National Security Council
Mr. Kevin Knott	TSA
Mr. Greg Kyrytschenko	Guardian Life

Name	Organization
Mr. Zach Landis	TSA
Mr. Tim Leaf	TSA
Mr. Nick Leiserson	Office of the National Cyber Director (ONCD), Executive Office of the President (EOP)
Mr. Ian Levy	Amazon
Mr. Robert Lord	CSD, CISA
Mr. Dhinesh Manoharan	Intel
Mr. Eric Mill	OMB
Mr. Ashok Misra	Microsoft
Lt Gen Charles Moore, USAF, Ret.	Former Deputy Commander, U.S. Cyber Command
Mr. Jeff Palomino	TSA
Mr. Joseph Pantoga	Krebs Stamos Group
Mr. Dylan Presman	ONCD, EOP
Ms. Sonya Proctor	TSA
Mr. Thomas Reagan	Marsh McLennan
Mr. Eric Rollison	Cybersecurity, Energy Security, and Emergency Response (CESAR), U.S. Department of Energy (DOE)
Mr. Sasha Romanosky	RAND
Mr. Tony Sager	Center for Internet Security
Mr. DJ Sampath	Cisco
Mr. Nick Saunders	Viasat
Mr. Adam Sedgewick	National Institute of Standards and Technology (NIST), U.S. Department of Commerce
Mr. Gary Seffel	TSA
Mr. Matt Scholl	NIST

Name	Organization
Mr. Chase Small	Krebs Stamos Group
Mr. Alex Stamos	Krebs Stamos Group
Mr. Josh Stankus	CSD, CISA
Mr. Kevin Stine	NIST
Mr. Jonathan Swanson	Krebs Stamos Group
Ms. Kiersten Todt	Former Chief of Staff, CISA
Mr. Phil Venables	Google Cloud
Mr. Tyler Warren	Prologis
Ms. Mara Winn	CESAR, DOE

Table 4: Management

Name	Organization
Ms. Christina Berger	President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer (DFO)
Ms. Joan Harris	Edgesource Corp.
Ms. Jennifer Poole	Edgesource Corp.
Mr. Wayne Rash	NSTAC ADFO
Mr. Nicholas Smith	TekSynap Corp.
Mr. Scott Zigler	NSTAC Alternate DFO

Appendix C. Acronyms

Table 5: Acronyms

Acronym	Definition
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
ADFO	Alternate Designated Federal Officer
AI/ML	Artificial Intelligence and Machine Learning
AICPA	American Institute of Certified Public Accountants
BOD	Binding Operational Directive
CCPA	California Consumer Privacy Act
CI	Critical Infrastructure
CIRCIA	Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
CNSSI	Committee on National Security Systems Instruction
CPGs	Cross-Sector Cyber Performance Goals
CSP	Cloud Service Provider
CSWG	Control Systems Working Group
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DOC	Department of Commerce
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy

Acronym	Definition
DOJ	Department of Justice
DOL	Department of Labor
EO	Executive Order
ERM	Enterprise Risk Management
ESG	Environmental, Social, and Governance
FedRAMP	Federal Risk Authorization Management Program
FERC	U.S. Federal Energy Regulatory Commission
FBI	U.S. Federal Bureau of Investigation
GSA	General Services Administration
GCC	Government Coordinating Councils
IAF	International Accreditation Forum
IAM	Identity and Access Management
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IIJA	Infrastructure Investment and Jobs Act
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
LoRa	Long-Range
LTE	Long-Term Evolution
MS-ISAC	Multi-State Information Sharing and Analysis Center
MOA	Memorandum of Agreement
NCCOE	National Cybersecurity Center of Excellence

Acronym	Definition
NCSR	National Cyber Security Review
NEC	National Economic Council
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSM	National Security Memorandum
NSPD	National Security Presidential Directive
NSTAC	President's National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OPM	Office of Personnel Management
OT	Operational Technology
PCI	Payment Card Industry
PLC	Programmable Logic Controllers
POA&Ms	Plans of Action and Milestones
ROI	Return on Investment
SaaS	Software-as-a-Service
SBOM	Software Bill of Materials
SCC	Sector Coordinating Councils
SEC	Securities and Exchange Commission

Acronym	Definition
SI	Systems Integrator
SOC	System and Organization Controls
SLTT	State, Local, Tribal, and Territorial
SP	Special Publication
SSDF	Secure Software Development Framework
SSH	Secure Shell Protocol
SSSCF	Secure Software Self-Attestation Common Form
U.S.	United States
U.S.C.	United States Code
USG	United States Government
ZTA	Zero Trust Architecture

Appendix D. Definitions

Table 6: Definitions

Term	Definition	Source
Active Directory	A Microsoft directory service for managing identities in Windows domain networks (registered trademark).	▪ National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-16B ▪ NIST SP 1800-16C ▪ NIST SP 1800-16D
Adversary	Any individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.	▪ NIST SP 800-30 ▪ CSRC | NIST
Artificial Intelligence	(1) A branch of computer science devoted to developing data processing systems that perform 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*
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.	▪ NIST Interagency or Internal Report (NISTIR) 8006, *NIST Cloud Computing Forensic Science Challenges*

Term	Definition	Source
Connectivity	Capacity for interconnecting platforms, systems, and applications.	▪ PCMag
Controlled Unclassified Information	Information that laws, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under *EO 13526: Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.	▪ NIST SP 800-171 Rev. 2 under controlled unclassified information from EO 13556 ▪ NIST SP 800-172 under controlled unclassified information from EO 13556 ▪ NIST SP 800-171 Rev. 1 [Superseded] under controlled unclassified information from EO 13556
Counterfeit	An unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source.	▪ NIST SP 800-161, 18 United States Code (U.S.C.)
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

Term	Definition	Source
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.	▪ Committee on National Security Systems Instruction (CNSSI) 4009-2015 from National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23) ▪ NIST SP 1800-25B ▪ NSPD-54/HSPD-23 ▪ NIST SP 1800-26B ▪ NSPD-54/HSPD-23 ▪ NIST SP 800-160 Vol. 2 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 ▪ NISTIR 7621 Rev. 1
Directory Services	A distributed database service capable of storing information, such as certificates and certificate revocation lists, in various nodes or servers distributed across a network. (Directory services stores identity information and enables the authentication and identification of people and machines.)	▪ NIST SP 1800-16B under Directory Service from NIST SP 800-15 ▪ NIST SP 1800-16D under Directory Service from NIST SP 800-15
Emerging Technologies	Technologies that are currently developing and are expected to impact society in some significant way over the next 5 to 10 years.	▪ Independence University

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
Fifth Generation	The fifth installment of advanced wireless technology, bringing about increased bandwidth and capacity for advancements within the Internet of Things.	▪ Qualcomm
Fourth Generation (4G)	A successor of the third-generation standards. A 4G system provides mobile ultra-broadband internet access, for example, to laptops with Universal Serial Bus wireless modems, smartphones, and other mobile devices.	▪ International Center for Applied Studies in IT
Hardware	The physical components of an information system.	▪ Hardware - Glossary | CSRC (nist.gov)
Identity and Access Management	(Also known as identity management.) A fundamental cybersecurity concept focused on ensuring "the right people and things have the right access to the right [technology] resources at the right time."	▪ NIST: Identity and Access Management

Term	Definition	Source
Industrial Control System (ICS)	A general term that encompasses several types of control systems, including supervisory control and data acquisition systems, distributed control systems, and other control-system configurations such as programmable logic controllers 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)	▪ CSRC | NIST
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

Term	Definition	Source
Infrastructure Investment and Jobs Act	Requires brokers to report to the Internal Revenue Service the cost basis of digital assets transferred by their clients to non-brokers, similar to how securities brokers report stock and bond trades.	▪ Small Business Association of Michigan
Internet of Things	Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation (as presented in NIST SP 800-183). IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision-making.	▪ NIST SP 800-183 ▪ Internet of Things - Glossary | CSRC (nist.gov)
Long-Term Evolution	Long-Term Evolution (LTE), commonly referred to as 4G, is a standard for nationwide public safety broadband. This standard allows access to digital technologies and deliver expanded capabilities in the field. The LTE standard supports fast speeds, with speeds up to 10 times faster than 3G networks.	▪ U.S. Department of Justice
Machine Learning	A branch of artificial intelligence focused on building applications that learn from data and improve their accuracy over time without being programmed to do so.	▪ Machine Learning | IBM
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 ▪ CSRC | NIST

Term	Definition	Source
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
National Vulnerability Database (NVD)	The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol. This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security-checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.	▪ National Vulnerability Database | NIST
Operating System	The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.	▪ NIST SP 800-44 Version 2 ▪ NISTIR 7621 Rev. 1 from NIST SP 800-44 Version 2

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
Sixth Generation	Sixth generation of wide-area wireless technology.	▪ PCMag

Term	Definition	Source
Software Application	A software program hosted by an information system.	▪ CNSSI 4009-2015 from NIST SP 800-37 Rev. 1 ▪ NIST SP 1800-16B under Application from NIST SP 800-137 ▪ NIST SP 1800-16C under Application from NIST SP 800-137 ▪ NIST SP 1800-16D under Application from NIST SP 800-137 ▪ NIST SP 800-137 under Application from NISTIR 7298 ▪ NIST SP 800-37 Rev. 2 ▪ NIST SP 800-53 Rev. 5 from NIST SP 800-37 Rev. 2 ▪ NISTIR 7621 Rev. 1 under Application from CNSSI 4009-2015 ▪ NIST SP 800-37 Rev. 1 [Superseded] under Application
Software Developers	A person or group that designs and/or builds and/or documents and/or configures the hardware and/or software of computerized systems.	▪ Food and Drug Administration, Glossary of Computer System Software Development Terminology (8/95)

Term	Definition	Source
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 denial of service.	▪ NIST SP 800- 53, CNSSI 4009, Adapted ▪ NIST: Threat
Threat Environment	The online space where cyber-threat actors conduct malicious cyber-threat activity.	▪ An Introduction to the Cyber Threat Environment
Trustworthiness	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.	▪ NIST SP 800-39, CNSSI-4009
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 ▪ ISO 9000 – Adapted ▪ NISTIR 7622 under Verification from CNSSI 4009, ISO 9000 – Adapted
Virtual Private Network	A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.	▪ NIST SP 800-113 under Virtual Private Network

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
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.	▪ Implementing a Zero Trust Architecture | NIST

Appendix E. Bibliography

Microsoft. "Microsoft Digital Defense Report Building and improving cyber resilience." October 2023. https://go.microsoft.com/fwlink/?linkid=2249025&clcid=0x409&culture=en-us&country=us

Cybercrime Magazine. "Global Cybersecurity Spending to Exceed $1.75 Trillion From 2021-2025." September 10, 2021. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

Securities and Exchange Commission. "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." March 9, 2022. https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf

The Big Newsletter. "How to Get Rich Sabotaging Nuclear Weapons Facilities." January 3, 2021. https://www.thebignewsletter.com/p/how-to-get-rich-sabotaging-nuclear

National Cybersecurity Center. "APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers." April 18, 2023. https://www.cisa.gov/sites/default/files/2023-04/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers-uk.pdf

Cybersecurity and Infrastructure Security Agency. "CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities." October 23, 2023. https://www.cisa.gov/news-events/alerts/2023/10/23/cisa-updates-guidance-addressing-cisco-ios-xe-web-ui-vulnerabilities

The Economic Times. "Tens of Thousands of Cisco Devices Compromised After Hackers Exploit Critical Bug." October 20, 2023. https://telecom.economictimes.indiatimes.com/news/devices/tens-of-thousands-of-cisco-devices-compromised-after-hackers-exploit-critical-bug/104582658

Cybersecurity and Infrastructure Security Agency. "Exploitation of Unitronics PLCs used in Water and Wastewater Systems." November 28, 2023. https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

Cybersecurity and Infrastructure Security Agency. "Cybersecurity Advisory: Scattered Spider." November 16, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

Federal Communications Commission. "FCC Proposes Cybersecurity Labeling Program for Smart Devices." August 10, 2023. https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-device

Garg, V., 2021, July. Covenants Without the Sword: Market Incentives for Cybersecurity Investment. In TPRC49: The 49th Research Conference on Communication, Information, and Internet Policy.

National Telecommunications and Information Administration. "Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program." August 16, 2013. https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf

Anderson, R. and Moore, T., 2006. The economics of information security. science, 314(5799), pp.610-613.

Cybersecurity and Infrastructure Security Agency. "Executive Order 13636: Improving Critical Infrastructure Cybersecurity." June 12, 2013. https://www.cisa.gov/sites/default/files/publications/19_1115_dhs-eo13636-analytic-report-cybersecurity-incentives-study%281%29.pdf

Cybersecurity and Infrastructure Security Agency. "Cyber Resource Hub." https://www.cisa.gov/cyber-resource-hub

National Security Agency. "Cybersecurity Collaboration Center." https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/

U.S. Cyber Command. "Private Sector Partnerships." https://www.cybercom.mil/Partnerships-and-Outreach/Private-Sector-Partnerships/

National Telecommunications and Information Administration. "National Cybersecurity Center of Excellence." https://www.nccoe.nist.gov/

The White House. "Office of Management and Budget Releases Draft Memorandum for Modernizing the Federal Risk and Authorization Management Program (FedRAMP)." October 27, 2023. https://www.whitehouse.gov/omb/briefing-room/2023/10/27/office-of-management-and-budget-releases-draft-memorandum-for-modernizing-the-federal-risk-and-authorization-management-program-fedramp/#:~:text=The%20proposed%20guidance%2C%20which%20would,Government.%20Development%20of%20the%20draft

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. https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf

Forrester. "The Rise of The Business-Aligned Security Executive." August 2020. https://static.tenable.com/marketing/whitepapers/Forrester-The_Rise_Of_The_Business-Aligned_Security_Executive.pdf

Cisco. "Cisco Cybersecurity Readiness Index." March 2023. https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf

National Telecommunications and Information Administration. "Integrating Cybersecurity and Enterprise Risk Management (ERM)." October 2020 https://csrc.nist.gov/pubs/ir/8286/final

FIAR Institute. https://www.fairinstitute.org/

National Institute of Standards and Technology. "The NIST Cybersecurity Framework 2.0." August 2023. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

Cybersecurity and Infrastructure Security Agency. "Cross-Sector Cybersecurity Performance Goals." July 21, 2023. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Cybersecurity and Infrastructure Security Agency. "CISA CPG Checklist." March 2023. https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

Chainalysis. "Crypto Crime Mid-Year Update: Crime Down 65% Overall, But Ransomware Headed for Huge Year Thanks to Return of Big Game Hunting." July 12, 2023. https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/#:~:text=In%20fact%2C%20ransomware%20attackers%20are,trailing%20only%202021's%20%24939.9%20million

American Institute of Certified Public Accountants. "CPA License Verification - Find a CPA." https://us.aicpa.org/forthepublic/findacpa

International Accreditation Forum. "IAF Certification Bodies." https://www.iafcertsearch.org/search/certification-bodies

National Skill Coalition. "Closing the Digital Skill Divide." February 6, 2023. https://nationalskillscoalition.org/resource/publications/closing-the-digital-skill-divide/

The White House. "National Cyber Workforce and Education Strategy." July 31, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

National Security Telecommunications Advisory Committee. "NSTAC Report to the President on a Cybersecurity Moonshot." November 14, 2018. https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf

United Nations. "Diverse, inclusive workplace: 'Key driver of resilience and recovery'." April 6, 2020. https://news.un.org/en/story/2022/04/1115672

World Economic Forum. "Why Cybersecurity Needs a More Diverse and Inclusive Workforce." October 26, 2021. https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/

Microsoft. "Why diversity is important for a strong cybersecurity team." September 9, 2021. https://www.microsoft.com/en-us/security/blog/2021/09/09/why-diversity-is-important-for-a-strong-cybersecurity-team/

Curry, S, Forbes. "Neurodiversity: A Competitive Advantage in Cybersecurity." May 13, 2019. https://www.forbes.com/sites/samcurry/2019/05/13/neurodiversity-a-competitive-advantage-in-cybersecurity/?sh=3495ac406265

Gitnux. "Cybersecurity Diversity Statistics." December 16, 2023. https://blog.gitnux.com/cybersecurity-diversity-statistics/

Forbes. "Prioritize Diversity In Your Cybersecurity Teams For Better Business Results." December 14, 2021. https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/14/prioritize-diversity-in-your-cybersecurity-teams-for-better-business-results/?sh=1d0425cd3d14

Momentive AI. "Key to Retaining Employees." https://www.momentive.ai/en/blog/dei-key-to-retaining-employees/

ISACA. "Cybersecurity Workforce Diversity—Including Cultures, Personalities and Neurodiversity." October 12, 2021. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/cybersecurity-workforce-diversity-including-cultures-personalities-and-neurodiversity

Olney, Matt, TALOS Intelligence. "Why Cybersecurity Needs a More Diverse and Inclusive Workforce." April 18, 2023. https://blog.talosintelligence.com/state-sponsored-campaigns-target-global-network-infrastructure/

Dawson, J.; R. Thomson; "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance," Frontiers in Psychology, 2018

Cybersecurity and Infrastructure Security Agency. "BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces." June 13, 2023. https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02