NASSCOM®

Comments Submitted by NASSCOM to the National Institute of Standards and Technology (NIST) on Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Submitted via www.regulations.gov

April 25, 2022

<u>Re: NIST Cybersecurity RFI - Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management (NIST-2022-0001)</u>

Dear Ms. Chambers,

The National Association of Software and Services Companies (NASSCOM), in association with Data Security Council of India (an initiative of NASSCOM) is submitting comments in response to the National Institute of Standards and Technology (NIST) Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management[1] (Docket No. NIST-2022-0001).

1. Introduction

NASSCOM is a global trade association with over 3,000 members, including virtually all the major U.S. technology companies and leading technology companies in other geographies. Our membership includes U.S. financial institutions and others outside the tech sector that have significant captive IT operations in India. Over 500 of our members are either headquartered or do significant business in the United States. NASSCOM members employ hundreds of thousands of workers in the United States and serve clients in every state and in virtually every sector of the U.S. economy. More than 75% of Fortune 500 companies and thousands of other entities in America rely on NASSCOM members for operational support, innovation, and assistance in navigating the digital transformations that are sweeping the business world. Throughout the COVID-19 pandemic, NASSCOM member companies have been providing critically needed "essential services" to financial institutions, hospitals, pharmaceutical and biotech companies and biotech companies, state and local government agencies, technology and communications firms, grocers, manufacturers, and thousands of other businesses across the U.S. Our companies deployed their best

[1] 87 Fed. Reg. 9579 (Feb. 22, 2022), https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

technology innovations to assist organizations across all sectors and people across the globe address and adapt to the serious challenges created by the pandemic.

NASSCOM's member companies are leaders across technology industries, providing software development, software design and system analysis, software products, IT-enabled/business process services, e-commerce services, engineering services, chip design, product development, internet, telecommunications, and manufacturing services to clients in every business sector throughout the global economy.

Data Security Council of India (DSCI) is a not-for-profit industry body on data protection in India, setup by NASSCOM. It is committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity building and outreach activities.

In these comments, we outline the evolving cyber threat environment in the current geo-political context, specific recommendations for improving the cybersecurity in supply chains, and provide use cases of Indian technology companies developing cutting edge cybersecurity solutions for their U.S. and global clients.

2. The evolving global cyber threat landscape

Today's dynamic geo-political and regulatory landscape has rendered traditional cybersecurity approaches irrelevant. Practices established when IT infrastructure components were located within a company's four walls are not sufficient in an era of cloud computing, Internet of Things (IoT), artificial intelligence (AI) and advanced analytics. The cyberattack risks faced by companies using outmoded security methods have increased dramatically during the COVID-19 pandemic. With most employees working remotely, sensitive data needs to be shared outside a company's walls. This includes employee data, intellectual property, corporate financial data, and other proprietary information. It also includes data on customers, their purchases, and the performance of products in the field.

Cybercriminals have seized this opportunity by launching phishing schemes that lure email users to click on malicious files. Many of these schemes have been COVID-19 related, and they have ranged from audio files impersonating voicemail targeting Office 365 users to emails purporting to be from company executives[2]. The number of remote desktop protocol (RDP) servers exposed to the internet increased from

[2] "COVID-19 Phishing Update: Voicemail Attacks Surface Targeting Office 365 Users," The PhishLabs Blog, https://www.phishlabs.com/blog/covid-19-phishing-update-voicemail-attacks-surface-targeting-office-365-users/.

3 million in January 2020 to more than 4.5 million in May, and attacks targeting them more than triple during March-April 2020 in the United States[3].

Further, bring-your-own-device (BYOD) work protocols allows cyber attackers to leverage outdated and unpatched operating systems or insecure apps on employee machines.[4] Employees themselves can pose risks, whether through poor cybersecurity hygiene or malicious intent. Deeply integrated partners and suppliers, including third-party vendors and their suppliers, can also serve as the link to criminal activities. For example, the 2013 Target data breach where hackers stole 40 million credit card numbers and personal details for 70 million customers began with malware used to steal login credentials from an HVAC subcontractor[5]. Criminals can also exploit numerous non-human entities, e.g., robots, automated functions, and technologies with system access, such as IoT devices and operational technology.

With so many susceptibilities involved, the extent of cyberattacks is on the rise. Marriott was attacked in April 2020, compromising the data of more than 5 million guests, its second major cyberattack in two years[6]. Also in April 2020, Energias de Portugal, one of Europe's largest electricity and gas providers, sustained a cyberattack with thieves demanding $11 million in ransom[7]. In some cases, criminals are targeting organizations integral to the pandemic response. Hacking attempts at the World Health Organization coronavirus testing lab doubled after the pandemic began[8]. In addition, hackers have targeted at least six pharmaceutical companies in the U.S., the U.K. and South Korea working on COVID-19 treatments[9].

Examining cyber incidents from January 2020 to early July 2021, the European Union Agency for Cybersecurity (ENISA) in its report, *Threat landscape for supply chain attacks*, found that around 62% of attacks targeted a supplier's system[10]. With an elevated state of cyber defenses and increased cybersecurity

[3] Lucian Constantin, "Attacks against internet-exposed RDP servers surging during COVID-19 pandemic," CSO (May 8, 2020), https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic html.
[4] Tamara Scott, "Cybersecurity Trends in 2020: BYOD and Mobile," Technology Advice (Jan. 7, 2020), https://technologyadvice.com/blog/information-technology/cybersecurity-trends-2020-byod-mobile/.
[5] David Lukic, "Target Data Breach, How Target Almost Lost Everything," ID Strong (Sep. 22, 2020), https://www.idstrong.com/sentinel/that-one-time-target-lost-everything/.
[6] Scott Ikeda, "Marriott Hit With Second Major Data Breach in Two Years; Over Five Million Guests Compromised," CPO Magazine (Apr. 13, 2020), https://www.cpomagazine.com/cyber-security/marriott-hit-with-second-major-data-breach-in-two-years-over-five-million-guests-compromised/.
[7] Doug Olenick, "Ragnar Locker's well-conceived ransomware attack on Energias de Portugal ," SC Media (Apr. 16, 2020), https://www.scmagazine.com/news/security-news/ransomware/ragnar-lockers-well-conceived-ransomware-attack-on-energias-de-portugal.
[8] Raphael Satter, Jack Stubbs, and Christopher Bing, "Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike," Reuters (Mar. 23, 2020), https://www reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN.
[9] Andrew Jeong, "North Korean Hackers Are Said to Have Targeted Companies Working on Covid-19 Vaccines," The Wall Street Journal (Dec. 2, 2020), https://www.wsj.com/articles/north-korean-hackers-are-said-to-have-targeted-companies-working-on-covid-19-vaccines-11606895026.
[10] "Understanding the increase in Supply Chain Security Attacks," ENISA (Jul. 29, 2021), https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.

awareness, threat actors are strategically targeting companies intertwined with the supply chains of large enterprises or government entities as the common attack vectors are rendered ineffective. Supply chain attacks exploit the inherently trusted relationship between vendors and customers or machine-to-machine communication channels, and a single attack can potentially put thousands of computers at risk across many companies or organizations.

Geopolitics has further compounded this already complex problem. Cyberattacks are increasingly playing a strategic role in geopolitical conflicts between States. Given the deep integration of global markets, escalations in the cyber domain could have economic implications across geographies and impact across industry verticals. Along with the use of military force, offensive campaigns also involves cyber-attacks on Government and critical infrastructure, mainly in a combat support role. There exist significant concerns of the possible spill-over of such cyberattacks globally, standing as a stark reminder of the havoc created by NotPetya ransomware attack in 2017 which crippled the operations of cross-industry multinationals like global transport and logistics giant Maersk, food and beverage manufacturer Mondelez, pharmaceutical giant Merck, advertising agency WPP, health and hygiene products maker Reckitt Benckiser, French construction company Saint-Gobain and FedEx's European subsidiary TNT Express[11].

Legacy cybersecurity solutions are not robust enough to secure a contemporary technology ecosystem consisting of remote workers, workplaces, partners and customer interactions, or to protect the data that employees may need to access at remotely. With the steady rise in digital adoption, new age technology applications like cloud computing, Internet of Things (IoT), artificial intelligence (AI), and the rise in data breaches, Governments and businesses need to consider the broader ecosystem and apply adaptable cybersecurity solutions that cater to dynamic challenges.

3. Specific Recommendations for Improving the Cybersecurity in Technology Supply Chains and Updating the NIST Cybersecurity Framework

Governments across the world are exploring ways to address vulnerabilities in supply chains critical to economic well-being and national security. India and the U.S. were among the top five most cyber-attacked nations in the world in 2019[12]. In this context, supply chain security risks in the information and communications technology (ICT) industry have received attention from both governments. Technology supply chain security is a subset of the overall cybersecurity concerns, however failure to adequately address these issues may have a significant impact on economic outcomes (international trade, commerce), political outcomes (trust in government), and social outcomes (trust in other institutions). The increased integration of software and hardware has exacerbated these concerns. As seen in the recent supply chain

[11] Rae Ritchie, "Maersk: Springing back from a catastrophic cyber-attack," About Us
I – Global Intelligence for Digital Leaders (Aug. 2019), https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

[12] The Global Threat Landscape Report 2019, Subex, https://www.subexsecure.com/the-global-threat-landscape-report-2019.

attack on SolarWinds[13], vulnerabilities in the software supply chain can have a pronounced impact on governments, the private sector, and consumers alike. Governments should not mandate specific technological solutions based on their location, nationality, or business models. Below we outline few design principles that could form the basis of boosting Cybersecurity in Technology Supply Chains and updating the NIST Cyber Framework.

The report of the 2019-21 UN Group of Governmental Experts[14] set forth few steps to ensure the integrity and security of technology supply chains. These include provisioning of national level frameworks and mechanisms; adoption of good practices and exchanges at the bilateral, regional, and multilateral levels; globally interoperable rules and standards; and inclusion of safety and security throughout the lifecycle of ICT products. Evaluating technology supply chain risks requires working closely with all partners, vendors and suppliers. Government and industry members should jointly execute this exercise of cyber supply chain risk assessment.

Accountability and verification are pivotal to ensuring the trustworthiness and integrity of cyber supply chain, which could be enabled through an industry-driven standard. It is important to benchmark software, hardware, equipment, and devices against security criteria, which could be leveraged by the stakeholders across the cyber supply chain, be it manufacturers, buyers, suppliers, system integrators, or service providers.

Further, modalities could be explored to enhance transparency and security in software development process, for example, via a standardized Software Bill of Materials (SBOM). A SBOM is an inventory of the components used in the development of a software product or service and their dependencies, used to keep track of every component employed in the development process. A SBOM has a utility for cyber supply chain security, providing an inventory of third-party or open-source components used in the software, firmware, or product. A standardized SBOM with defined baseline attributes and standardized formats and identification schemes could go a long way in supporting this effort.

An essential element in software supply chain security is to source technology from trusted vendors. This could be operationalized through a mechanism to develop a shared list of trusted or accredited vendors for technology products and services. This could be extended to vendor assessment, which includes evaluation of its data processing capabilities, security measures, incident response models, monitoring capabilities, etc.

[13] Lucian Constatin, "SolarWinds attack explained: And why it was so hard to detect," CSO (Dec. 15, 2020), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared html.
[14] Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security. https://dig.watch/updates/un-gge-20192021-publishes-advance-copy-final-report

Finally, traceability is vital to establish the origin and authenticity of software and hardware building blocks, components, and systems in the final product/deliverable. An auditable cyber supply chain is the cornerstone of trust and transparency in cyber products, and it could be enabled with the use of blockchain. Stakeholders across the cyber supply chain can track components and products as they move along the value chain.

The NIST Cyber Security Framework provides five overarching conceptual terms: Identify, Protect, Detect, Respond, and Recovery. The framework gave security managers purpose and direction to align security to real risks. More importantly, it underlined the need for preparation for the eventualities that are bound to happen in the rising scale, complexity, and pace of digitization. If NIST is looking at revisiting the framework, the points need deliberations and reflection:

- With the backdrop of expanding digital footprint and surfaces providing entry points for the attack vectors, active monitoring and management of this expanding surface must be significantly elevated in the framework.
- Operations and governance on a real-time basis are key to ensuring that issues with the potential for significant ramifications are addressed. A framework for the next decade should emphasize real-time operations and governance.
- The ability to get hold of the situation that could lead to a security issue is critical to managing security in the contemporary age. It should also trigger desired, proportionate, and timely action to limit the damage and recovery from the incident. The framework could give significant emphasis to policy governed handling of security.
- Ability to think of all possibilities, get hold of them, go to the desired level of depth, and ensure attention to each element in a coordinated way for synthesized and collective delivery of value to security preparedness, response, and governance. The idea of security orchestration offers this. The upcoming framework could try to give a reflection on this vital capability.
- Security is now increasingly dependent on the underlying capabilities than specific control. Underlying capabilities ensure coverage, offer desired level of accuracy, consume intelligence, keep up with the rising pace, address complexity and diversity, and satisfy performance requirements. The time has come to focus on them and articulate them better in the security framework.
- The volume and velocity of development and deployment of new solutions, software, or systems are rising significantly. Hence, the framework could suggest credible security interventions required for Development Operations (DevOps).
- Transaction processing is increasingly unbundled to leverage the global capabilities, components, and products. Focus on the security of the chain of products leveraged for transaction processing should get significant attention from the emerging security frameworks.
- Modernization of underlying infrastructure is changing the way applications are developed and deployed, containers, and microservices. The framework should be able to drive the overhauling of enterprise security for such modernization.

- The security managers have to take care of dimensions, nuances, granularities, and possibilities. They are responsible for enabling innovation, providing a better customer experience, and making security frictionless. They have to deal with rising interdependence, scale, and complexity. They have to be mindful of the situations and macro context shaping them. They have to find ways in the constrained resources and enhance the productivity of their efforts and investment. The security framework should deal with these elements cautiously to create a key differentiator.
- Managing the affairs of security demands work on activities like discovering, finding, identifying, recognizing, categorizing, contextualizing, distinguishing, characterizing, interpreting, mapping, configuring, administering, measuring, monitoring, prioritizing, prioritizing, and so on. The framework should provide overarching and representative themes to cover the wide range of activities required to perform for security.

4. Use cases of Indian technology companies developing cutting edge cybersecurity solutions for their global/ U.S. clients

Indian technology companies enable the necessary cyber capabilities availability and adoption for their global clients. Their portfolio of targeted technology offerings, talent pool and prior experience, are driving high business value for their enterprise clients and enable them to deal with the growing cyber threats effectively using in a boundary-less digital environment. Below we provide a few illustrative examples of NASSCOM member companies developing specific solutions to address cyber threats faced by their global/ U.S. clients.

Tata Consultancy Services (TCS) defined the security posture of a global energy major by automation of security operations and modernizing identity and access management. The client company was faced with sub-optimal IT security processes and policies, disparate processes and redundant legacy systems, posing a threat to its business performance. TCS prepared a multi-year roadmap to modernize and automate security operations, identity and access management processes, improve user experience and integrate processes and technologies. The implementation of a scalable and efficient identity and access management solution helped the client harmonize 11 disparate systems to a single system of records, also establishing automated user provisioning, mailbox, and personal drives for 25,000 users. By improving the efficiency of the process of performing patch management, TCS helped identify critical assets and reduce vulnerability of the most critical zones. This resulted in $1.5 million in cost avoidance for the client company with license optimization, $170K per year cost benefit, 100% remediation of demilitarized zone vulnerabilities and 70% Windows-based historic vulnerabilities for a 40% overall risk reduction and 40% more operational stability[15].

[15] "Energy Major Adopts Managed Security Services," https://www.tcs.com/services/cyber-security-future-ready-enterprise/customer-story/success-story/enterprise-security-identity-access-management.

Infosys worked with a global financial service provider to transform its Identity Access Management (IDAM) for stronger security and enhanced user convenience. In the post-pandemic world with remote working and the proliferation of smart devices, IDAM has become increasingly critical, especially for enterprises handling sensitive data. The client was grappling with multiple problems owing to its legacy system. Infosys streamlined the client's IDAM processes by enhancing security and productivity while reducing effort for access provisioning. Infosys also brought in efficiencies and convenience to client users by deploying modules such as user management, centralized data governance, bulk access approvals, and self-service access management. This resulted in enhanced user productivity by 70%, achieved 85% effort reduction through streamlined access management, and delivered 70% greater efficiency in data collection[16].

Mphasis helped a U.S.-based multinational pharmaceutical corporation to implement secured Protected Healthcare Information (PHI) as required by HIPAA and HITECH. The client faced challenges like data breaches and internal data leaks within the environment, ~1,500 applications not integrated to the existing IAM platform and being managed manually, no tracking mechanism for the individual SSL certificates expiration date resulting in business downtime, and aggressive deployment deadlines leading to incorrect coding and increased vulnerabilities. Mphasis deployed data leak solution complying to HIPAA and HITECH, reduced the data breaches through intelligent vulnerability prioritization, implemented workflow automation for on boarding, decommissioning and renewal process and on-boarded 1,500 high risk applications on IDAM platform and integrated through SSO. As a result, the client benefited from RBAC and data privacy, web-based reporting of all identified exploits and remediation status, user on boarding within 24 hours and de-provisioning within 30 minutes and operational cost optimization[17].

L&T Infotech (LTI) enabled business-critical data protection for a leading U.S. professional services firm. The client needed to protect their data at rest and conform to industry-specific compliance standards, and required expertise in data security to assess the existing data security solution from Thales and optimize it to protect their business critical data. LTI enabled quick availability of data security consultants both onsite and offshore to the client and prepared a detailed deployment plan. This included extensive stakeholder coordination including application owners, developers, database administrator, and IT support. LTI ensured successful implementation and testing of encryption project, effective BAU support and request fulfillment. Consequently, lower risk posture of critical business data was achieved by ensuring protection of 95% of data at rest with LTI's speed-to-market delivery capability, optimized cost of security operations with

[16] "Infosys Transforms Equatex's Identity Access Management for Stronger Security and Enhanced User Convenience," https://www.infosys.com/services/cyber-security/documents/access-management-stronger-security.pdf.
[17] "Pharmaceutical Firm Enabling Threat Justified Security Operations," https://www mphasis.com/home/services/cyber-security/case-study/pharmaceutical-firm-enabling-threat-justified-security-operations html.

seamless project implementation within three months for 250 database servers and ensured client meets the required compliance standards vis-à-vis data security, as per industry guidelines[18].

HCL Technologies helped a major U.S. energy company implement a comprehensive GRC solution. The client was facing the challenge of complying with a number of demanding and intersecting regulatory requirements. It strived to improve and refine GRC practices across the organization, ensure compliance framework integrity, and adhere to industry standards. Subsequently, top-level requirements for a services partner were established, including the ability to analyze current GRC processes and reform them. HCL presented a future-ready roadmap before the client initiated the implementation program, and simultaneously delivered inputs for resolving potential challenges. As a result, 50% saving on the cost of the program was achieved, duly recognized by the client. Other benefits included integration of all risk and compliance-related information, best practices implementation across a spectrum of functional areas, enterprise view of risk and the related management capability, and overall improvement of reporting capabilities and processes[19].

Tech Mahindra managed Security Services and DevSecOps for an international publishing company. The client needed to manage its cloud services for applications and cloud infrastructure, enhance the security posture in application development life cycle and provide managed security services. Tech Mahindra performed a due-diligence of the existing security controls deployed by the client, and then proposed the security controls to improve an application security and development life cycle by adopting DevSecOps model. As part of the DevSecOps cycle, Tech Mahindra performed Threat Modelling while building application architecture, integrated secure code scanning and application vulnerability scanning through CI/CD pipeline for continuous scanning and Runtime Application Self-Protection. This enabled the client to protect its customer cloud environment using multi-layered defense, enhanced security posture, cloud compliance and configuration management, proactive threat management through vulnerability assessment services and a streamlined process for vulnerabilities' remediation and patching cloud services[20].

5. Concluding Remarks

The risk of cyber-attacks has never been higher due to increased digital connectivity driven by a widespread adoption of new age technologies e.g., cloud computing, Internet of Things (IoT), Artificial Intelligence (AI) and advanced analytics. Attackers now have more sophisticated cyber tools and resources at their

---

[18] "Protecting Business-Critical Static Data for a Leading US Professional Services Firm," https://www.lntinfotech.com/wp-content/uploads/2021/07/Protecting-Business-Critical-Static-Data-for-a-Leading-US-Professional-Services-Firm.pdf?pdf=download.

[19] "HCL helped a major US energy company implement a comprehensive GRC solution - An Ovum case study," https://www.hcltech.com/success-story/cyber-security/hcl-helped-major-us-energy-company-implement-comprehensive-grc-solution.

[20] "Managed Security Services and DevSecOps for an International Publishing Company," https://files.techmahindra.com/static/img/pdf/security-services-for-publishing-company.pdf.

disposal. With an elevated state of cyber defences and increased cybersecurity awareness, threat actors are strategically targeting companies intertwined with the supply chains of large enterprises or government entities as the common attack vectors are rendered ineffective. Supply chain attacks exploit the inherently trusted relationship between vendors and customers or machine-to-machine communication channels, and a single attack can potentially put thousands of computers at risk across many companies or organizations.

Since cyber supply chains are dispersed globally, an effective response is rooted in close cooperation over shared and interoperable solutions among like-minded countries. Given the prominent role of the Indian technology industry in the U.S. software/ technology supply chains, collaboration across various cybersecurity fields could substantially boost the overall U.S.-India bilateral and strategic partnership. This is particularly relevant in light of skills shortages in the U.S., the invaluable role of both Indian technology companies as well as Indian technology professionals' play in the U.S., and the unique and trusted U.S.-India partnership on these issues. Research and development of cybersecurity technologies is a key area for collaboration, e.g., digital security, supply chain security, IoT/ hardware security, Cryptography, and Cryptanalysis. Specific research use cases could include AI-based incident response technologies and processes for combating ransomware attacks on critical infrastructure, decentralized identity technologies, AI and deep learning-based threat hunting techniques, research in areas of critical infrastructure resilience, Malware resistant operational systems for protecting national assets especially power, water and refinery, to name a few. Cybersecurity regulation is another important collaboration area, e.g., jointly develop a framework for threat intel sharing principles and opening up security data sets by both Governments for Innovation and Research. Finally, partnering on building Cybersecurity Talent, Skilling & Standards e.g., jointly accelerating cybersecurity skilling and certifications across government to tackle new age cybercrimes like nation-state threats, critical infrastructure and supply-chain attacks, ransomware, credentials theft, elections attacks, et al. could be a great step to boost the cybersecurity talent pool in both countries. This is particularly relevant in light of the skills shortages in the U.S., the invaluable role of both Indian technology companies as well as Indian technology professionals' in working with various U.S. and global enterprises across America, and the unique and trusted U.S.-India partnership on these issues.

NASSCOM is pleased to provide our inputs and we would welcome an opportunity to discuss our suggestions and next steps with your agencies.

Sincerely,

Shivendra Singh

Shivendra Singh
Vice President
NASSCOM

National Association of Software & Services Companies

Plot Number: 7-10, Sector – 126
Noida – 201303, India

T: [redacted]
F: [redacted]

www nasscom.in