Testimony of

Mr. Matthew A Scholl.
Chief
Computer Security Division
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Technology
and
Subcommittee on Investigations and Oversight

"SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains"

May 25, 2021

Chairwoman Stevens, Ranking Member Waltz, Chairman Foster, Ranking Member Obernolte and Members of the Subcommittee, I am Matthew Scholl, the Chief of the Computer Security Division, of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology – known as NIST. Thank you for the opportunity to testify today on SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains, which is of critical importance to the security and economic well-being of America.

NIST is home to five Nobel Prize winners, with programs focused on national priorities such as artificial intelligence, advanced manufacturing, the digital economy, precision metrology, quantum science, biosciences and, of course, cybersecurity. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST has a long history of working in support of cybersecurity including securing the nation's supply chains. There are many risks that need to be managed in supply chains. This includes availability of product, shipping, component availability, quality, interoperability, costs, delivery and now –more than ever – cybersecurity. As we have gotten better at understanding threat actors, managing cybersecurity risks and identifying vulnerabilities, our adversaries have improved their ability to compromise the confidentiality, availability and integrity of our information and information systems. Recent threat activity has highlighted the IT supply chain as one of these vulnerabilities. The ability to participate in the digital economy is available to almost everyone who can write software and participate in an opensource project. This enables the world to benefit from innovation, entrepreneurial spirit, expertise, and imagination at a scale never before seen, but the risks need to be understood and managed along with these benefits.

Organizations increasingly rely on an array of suppliers to support their critical functions and business missions. All organizations rely on acquiring products and services, and most organizations also supply products and services to individuals, groups, or other organizations. Supply chain management is an established discipline and is one of the key capabilities for enabling economic growth. These trends have resulted in organizations that no longer fully control the supply ecosystems of the products that they produce and procure, or the services that they rely on or deliver.

Cybersecurity risks associated with extended supply chains and supply ecosystems are significant, and those risks are difficult to understand by many organizations as they continue to expand their use of digital technologies to support critical functions or create digital products for their customers.

President's Executive Order on Cybersecurity – EO 14028

To address the ever-challenging issues related to cybersecurity, on May 12th, President Biden signed a critical Executive Order to improve the nation's cybersecurity and protect federal government networks. Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident that we are discussing at this hearing are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. These incidents share commonalities,

including insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to incidents.

The President's Executive Order makes a significant contribution toward modernizing cybersecurity defenses by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. It is the first of many ambitious steps the Administration is taking to modernize national cyber defenses. However, the Colonial Pipeline incident is a reminder that federal action alone is not enough. Much of our domestic critical infrastructure is owned and operated by the private sector, and the tools and resources NIST produces can be used by the private sector when determining their own cybersecurity risk and the management of that risk throughout supply chains.

Specifically, section 4 of the order directs the Secretary of Commerce, through NIST, to solicit input from federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security. NIST's work will address identifying and securing critical software, secure software development lifecycles and secure development environments, security measures for federal government, and requirements for testing software.

The EO assigns additional responsibilities to NIST, including initiating two pilot labeling programs related to secure software development practices and the Internet of Things to inform consumers about the security of their products. NIST will conduct these programs working closely with other government agencies and private and public sector organizations and individuals through our open, transparent and inclusive processes. Our goal is to respond to these responsibilities in ways that are effective in reducing risks to our software supply chains while continuing to facilitate the innovation and economic growth that a secure software ecosystem can provide.

NIST's arsenal in the defense against cyber attacks is large and growing. The rest of my testimony will cover the tool and products we have developed in support of the nation's strong cyber stance.

NIST's Role in Cybersecurity

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the Data Encryption Standard, which enabled efficiencies with security, like the electronic banking that we all enjoy today. NIST's role is to provide standards, guidance, tools, data references, and testing methods to protect information systems against threats to the confidentiality, integrity, and availability of information and services. This role was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-the-art, and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

Cyber Supply Chain Risk Management

When a device's supply chain is compromised, its security can no longer be assured, whether it is a chip, laptop, server, or any other technology. NIST is responsible for developing reliable and practical standards, guidelines, tests, and metrics to help organizations with their Cyber Supply Chain Risk Management (C-SCRM). The private and public sector can use these NIST-produced resources to create and conduct Cyber Supply Chain Risk Management Programs. That includes organizations developing or using information, communications, and operational technologies that depend upon complex, globally distributed, and interconnected supply chains. These supply chains cover the life cycle of technology—from research and development, design, and manufacturing to acquisition, delivery, integration, operations and maintenance, and disposal.

NIST's Cyber Supply Chain Risk Management Program

Managing cyber supply chain risk requires ensuring the integrity, security, quality, and resilience of the supply chain and its products and services. In order to assure this, NIST focuses on:

- **Foundational Practices**: C-SCRM lies at the intersection of information security and supply chain management. Existing supply chain and cybersecurity practices provide a foundation for building an effective risk management program.
- **Enterprise-Wide Practices**: Effective C-SCRM is an enterprise-wide activity that involves each tier (Organization, Mission/Business Processes, and Information Systems) and is implemented throughout the system development life cycle.
- **Risk Management Processes**: C-SCRM should be implemented as part of overall risk management activities. That involves identifying and assessing applicable risks and determining appropriate response actions, developing a C-SCRM Strategy and Implementation Plan to record selected response actions, and monitoring performance against that plan.
- **Critical Systems**: Cost-effective supply chain risk mitigation requires organizations to identify those systems/components that are most vulnerable and will cause the largest organizational impact if compromised

NIST has collaborated with public and private sector stakeholders to research and develop C-SCRM tools and metrics, producing case studies and widely used guidelines on mitigation strategies. These multiple sources reflect the complex global marketplace and assist federal agencies, companies, and others to manage supply chain risks which threaten their information

systems and organizations. The SECURE Technology Act and FASC Interim Final Rule gave NIST a specific role in developing C-SCRM guidelines.

Focusing on federal agencies – while also engaging with and providing resources useful to other levels of government and the private sector – NIST:

- Produced *Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161)* to guide organizations in identifying, assessing, and responding to supply chain risks at all levels. It is flexible and builds on organizations' existing information security practices. NIST is currently updating this primary technical resource using feedback from federal and industry partners.
- Participates in the Federal Acquisition Security Council, or FASC, created by law in 2018. The Council is authorized to develop policies and processes for agencies to use when purchasing technology products and services, and to recommend C-SCRM standards, guidelines, and practices that NIST should develop.
- Issued *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks (NISTIR 8272)*, which describes a prototype solution for filling the gap between an organization's risk appetite and supply chain risk posture by providing a basic measurement of the potential impact on a cyber supply chain.
- Released *Criticality Analysis Process Model: Prioritizing Systems and Components (NISTIR 8179)*, aimed at identifying systems and components that are most vital and may need additional security or other protections.
- Finalized *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (NISTIR 8276)*, summarizing practices foundational to an effective C-SCRM program.
- Hosts the Federal C-SCRM Forum, which fosters collaboration and the exchange of information among federal organizations to improve the security of their supply chains. It includes those responsible for C-SCRM in the federal ecosystem, among them the Office of Management and Budget (OMB), Department of Defense (DOD), Office of the Director for National Intelligence (ODNI), Cybersecurity and Infrastructure Security Agency (CISA), General Services Administration (GSA), and NIST.
- Co-leads the Software and Supply Chain Assurance Forum with DOD, the Department of Homeland Security (DHS), and GSA. The Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

Software Security

NIST provides a series of documentary guidance, data references, tools and testing as part of its program to work on improving the efficiency, reliability and security of software. Below are highlighted a few of these items that are used across the different areas of a software lifecycle.

The National Vulnerability Database

Protecting information technology is critical and NIST plays a key role in this area by maintaining the repository of all known and publicly reported information technology vulnerabilities, called the National Vulnerability Database (NVD). The NVD is an authoritative source for standardized information on security vulnerabilities that NIST updates regularly.

The vulnerabilities catalogued in the NVD are weaknesses in coding found in software and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. The NVD tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities.

The NVD is the second most frequently accessed website at NIST, after the NIST time service, and is used across the country by the IT and cybersecurity industry, by cybersecurity tools and scanners, by other nations and by computer emergency response teams around the world.

National Software Reference Library

NIST hosts the National Software Reference Library (NSRL). The NSRL creates digital signatures of software so that an organization can efficiently search its networks for that software and determine if and where the software is deployed.

The NSRL collects software from various sources and incorporates profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and private industry to review files on a computer by matching profiles in the RDS. This process helps alleviate much of the effort involved in determining which files on a computer are important forensics evidence.

Businesses and government agencies both use the NSRL RDS as part of their routine IT operations to ensure there are no malicious or unverified files on their systems.

Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

NIST, working with multiple partners across the software industry, wrote a white paper that recommends a core set of high-level secure software development practices called a secure software development framework (SSDF) that can be integrated with any software development lifecycle. This paper facilitates communications about secure software development practices among business owners, software developers, project managers and leads and cybersecurity professionals within an organization.

Software Assurance Metrics And Tool Evaluation (SAMATE)
The NIST SAMATE project is dedicated to improving software assurance by developing methods to enable software tool evaluations, measuring the effectiveness of tools and techniques, and identifying gaps in tools and methods. The scope of the SAMATE project is broad, ranging from a periodic evaluation of static analysis tools to improving the understanding of software bugs to formal methods and AI-enabled bug finding.

Software Assurance Reference Dataset (SARD)
SARD provides users, researchers, and software security assurance tool developers with a set of known security flaws. This allows end users to evaluate tools and tool developers to test their methods. The dataset includes "wild" (production), "synthetic" (written to test or generated), and "academic" (from students) test cases. This database also contains real software application with known bugs and vulnerabilities. The dataset includes a wide variety of possible vulnerabilities and languages.

National Cybersecurity Center of Excellence (NCCoE)
Established in 2012, NIST's National Cybersecurity Center of Excellence (NCCoE)[2] is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges.

Through consortia under Cooperative Research and Development Agreements, including private sector collaborators—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. Working with communities of interest, the NCCoE produces practical cybersecurity solutions that benefit large and small businesses, and third-party service providers in diverse sectors.

The NCCoE has many published practice guides, on-going projects exploring solutions, and upcoming projects exploring new challenges and building communities of interest that all directly support many of the cybersecurity issues we have today. There are several projects focused on supply chain security that are currently underway at the NCCoE. One of these projects is aimed at identifying methods to help organizations verify that the internal components (chips) of purchased computing devices are genuine and have not been altered during the devices' lifecycle (from manufacturing to distribution, after sale from a retailer, and until the device is retired from service). Another project is working to demonstrate effective and efficient methods to patch software in a managed enterprise.

Conclusion
Our economy is increasingly global, complex, and interconnected. It is characterized by rapid advances in information technology. IT products and services need to provide sufficient levels

[2] https://www.nccoe.nist.gov/

of cybersecurity and resilience. The timely availability of international cybersecurity standards and guidance is a dynamic and critical component for the cybersecurity and resilience of all information and communications systems and supporting infrastructures.

The NIST's C-SCRM program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of information and information systems. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

NIST is proud of its role in establishing and improving the set of cybersecurity technical solutions, standards, guidelines, and best practices, and of the longstanding and robust collaborations we've established with our federal government partners, private sector collaborators, and international colleagues. Supply chain risk management is a complex issue that is not solely a cybersecurity problem, but an issue that needs to be addressed at an enterprise level. NIST is committed to applying its core values of excellence and persistence as we work with all of our stakeholders to continuously improve NIST standards, guidance, tools and other resources, and to identify new resources to help solve the critical issues facing our nation.

Thank you for the opportunity to present NIST's activities on C-SCRM and software assurance. I will be pleased to answer any questions you may have.

Matthew A Scholl

Matthew Scholl is the Chief of the Computer Security Division (CSD) in the Information Technology Laboratory (ITL) at the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). CSD, one of seven Divisions within ITL, has an annual budget of $32 million, nearly 100 federal employees, and an additional approximately 50 guest researchers from industry, universities, and foreign laboratories.

Mr. Scholl oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry.

He also co-leads NIST's participation with Cybersecurity National and International Standards Development Organizations (SDOs) and associated conformance testing programs.

Mr. Scholl has a Master's in Information Systems from the University of Maryland and a bachelor's degree from the University of Richmond.

He is a U.S. Army veteran and currently has more than 20 years of federal service.