October 2021

MEMO

To: Interested Parties
From: Information Technology Industry Council (ITI)
Re: 2022 Global Cybersecurity and Supply Chain Outlook

Protecting digital infrastructure and systems through enhanced cyber and supply chain security is a priority for both private sectors and governments worldwide and has increasingly become an integral part of national security discussions. As countries consider varying proposals, it is important that they work to increase security while promoting innovation, maintaining the benefits cyberspace provides, and reflecting the interconnected and interoperable global nature of today's digital environment. Further, it will be critical for cyber and supply chain security policies to be adaptable to respond to rapidly evolving threats and technologies; be grounded in effective risk management principles, and leverage public-private partnerships.

Looking ahead to 2022, we will continue to see policymaking activities on cyber and supply chain security and resiliency, including Internet of Things (IoT) certification and labeling, security incident reporting, the security of telecommunications networks including 5G, and zero trust remain prominent. Below, we offer ITI's global cybersecurity outlook with key issues to watch in various strategic markets.

United States

Executive Order on Improving the Nation's Cybersecurity

In May 2021, the Biden Administration published the *Executive Order on Improving the Nation's Cybersecurity* initiating a government-wide effort to enhance the U.S. national posture on cybersecurity with numerous tasks, deliverables, and requirements. Many of these provisions will directly impact federal contractors' practices on removing barriers to sharing threat information, modernizing federal government cybersecurity, and enhancing software supply chain integrity. They are also likely to affect commercial practices of federal contractors and may therefore establish broader precedent. Since the release of the Executive Order (EO), ITI submitted comments to identify standards and best practices for enhancing software supply chain security, highlighting the importance of international standards and taking a risk-based approach for critical software. Additionally, ITI submitted comments to encourage the administration to approach software supply chain issues in a holistic manner as it considers Software Bill of Materials (SBOMs) minimum elements. SBOMs are an important transparency tool, but should not be misconstrued as a mechanism to provide secure software development practices.

In its effort to guide the U.S. government towards adopting a Zero Trust approach to cybersecurity, the Office of Management and Budget (OMB) plans to promote the vigorous use of modern technology and security practices. ITI commented on a National Institute of Standards and Technology Zero Trust Starting Guide for Administrators, and submitted comments to OMB highlighting the importance of aligning the targeted end-state to use cases rather than technology silos, and identifying gaps and inconsistencies for a federal zero trust strategy. The EO also recommends stronger cybersecurity practices beyond the federal government space as it directs two pilot programs on cybersecurity labeling for IoT devices and consumer software to educate the public on the cybersecurity capabilities in IoT devices and software development practices. To ensure labeling does not convey a false sense of security, ITI submitted comments highlighting both consumers and vendors must understand their respective roles in maintaining cybersecurity by leveraging ITI's first-of-its-kind Cybersecurity Labeling Policy Principles.

In 2022, we will continue to see various U.S. government agencies carry out implementing tasks pursuant to the Cybersecurity EO. For Q1, we expect the release of guidance on improving software supply chain security as well as the official launch of the consumer labelling pilots for IoT Security and Secure Software Development. For Q2, we anticipate the release of additional procedures to review standards relating to software supply chain security as well as the publication of standardized contracting language to protect critical software. Given that various government agencies have done the majority of the EO tasks this year, it is crucial to see how the Federal Acquisition Regulatory (FAR) Council would work with other government partners to implement these cybersecurity requirements in the federal procurement space. The launch of the consumer labeling program creates an opportunity for vendors and consumers to assess the effectiveness of the program and learn from their experience.

Executive Order on America's Supply Chains

In February 2021, the Biden Administration released the *Executive Order on America's Supply Chains*, which directed a whole-of-government approach to assess vulnerabilities and strengthen resilience of critical supply chains in four areas: semiconductor manufacturing and advanced packaging, large capacity batteries, critical minerals and materials, and pharmaceuticals. The U.S. Department of Commerce Bureau of Industry and Security's (BIS) 100-Day Review Report on Semiconductors offered several recommendations for the U.S. to build resilient supply chains, revitalize American manufacturing, and foster broad-based growth by working with industry stakeholders. The recommendations in the report largely aligned with ITI's comments to the Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain. In 2022, semiconductor supply chain resiliency will likely stay as one of the priorities for the administration and the U.S. has an opportunity to conduct more international engagements on semiconductors to form consensus and adopt common approach to strengthen the supply chain.

Beyond this specific focus on semiconductors, the administration continues to prioritize broader information and communications technologies (ITC) supply chain risk management. The America's Supply Chains EO further requires the Secretaries of Commerce and Homeland Security to submit a report to the president to review supply chains for critical sectors and subsectors of the ICT industrial base, including hardware, software, data, and associated services, within one year. Additionally, the Interim *Final Rule to Secure the Information and Communications Technology and Services Supply Chain* came into effect in March 2021. It allows the Secretary of Commerce to block or unwind transactions with a "foreign adversary" deemed to pose an undue risk. To help address policymakers' concerns regarding risks to the global ICT supply chains, ITI continues to leverage our Supply Chain Security Policy Principles to advocate for a clear, narrow scope regarding the ICTS Supply Chain IFR, and provide useful feedback to the request for public comments on Risks in the Information Communications Technology Supply Chain. Additionally, ITI testified before the Senate Committee on Science, Commerce, and Transportation on supply chain resiliency, focusing on the need for government and industry collaboration on a coordinated approach, including leveraging the Department of Homeland Security ICT Supply Chain Risk Management Task Force as the convening force for public-private partnership on ICT supply chain security issues. In 2022, the ICT supply chain security issue is prominent, as the technology supply chain continues to be intertwined with national security and economic competitiveness.

Cyber Incident Reporting

Recent cybersecurity incidents such as the SolarWinds compromise and the Colonial Pipeline ransomware attack have brought cybersecurity into sharp focus in the United States and globally. Policymakers around the world have increasingly turned to incident reporting regimes as a potentially appropriate tool to gain greater visibility into such compromises. In the United States, Sens. Mark Warner (D-VA), Marco Rubio (R-FL), and Susan Collins (R-ME) introduced the *Cybersecurity Incident Notification Act of 2021*. Additionally, Reps. Yvette Clarke (D-NY) and John Katko (R-NY) are developing the *Cyber Incident Reporting for Critical Infrastructure Act of 2021*, which has been adopted by the Senate Homeland Security Committee led by Senators Gary Peters and Rob Portman. To inform the direction a mandatory cybersecurity incident reporting regime takes in the U.S, ITI testified before the House Committee on Homeland Security; and developed and released its Principles for Cyber Incident Reporting in the United States covering a range of issues, including differentiating between the concepts of cybersecurity incident reporting, threat information sharing, and data breach notification. ITI also released a set of Global Security Incident Reporting Policy Principles given the significant ongoing global policy conversation. The cybersecurity incident reporting topic is likely to remain a priority in the U.S. cybersecurity debate in 2022 given that it plays an important role in informing actions to respond to incidents and prevent further impacts.

Europe

NIS 2 Directive

The EU Cybersecurity Strategy first directed the European Commission to propose the Network and Information Security Directive in 2016 as the first piece of EU-wide cybersecurity legislation. To reflect the current cybersecurity landscape, a new version of the draft NIS 2 Directive was proposed in December 2020, on which ITI filed comments and held an event to discuss the draft proposal with Bart Groothuis, the lead Member of the European Parliament on the file. The NIS 2 Directive covers a wide range of topics on cybersecurity across the EU, including establishing a mandatory incident reporting regime, as well as provisions related to supply chain security, WHOIS data, cybersecurity certification, supply chain security, vulnerability disclosure, and enforcement and harmonization, among others. In October 2021, the European Parliament will vote on the various amendments, while the Council of the EU member states are working in parallel on its position. Once the European Parliament and the Council of the EU have finalized their respective positions, they will negotiate the final text of the NIS2 Directive, expected in 2022. It is crucial to watch how the NIS 2 Directive can serve as a convening and harmonizing force to raise the cybersecurity standard across Europe, while avoiding potential overlaps with other European laws and sectoral regulations.

EU Cybersecurity Act

To shape Europe's digital future, the 2019 EU Cybersecurity Act strengthens the EU Agency for Cybersecurity (ENISA) but also establishes a cybersecurity certification framework for ICT products and services. The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. While ENISA has not released a comprehensive cybersecurity certification roadmap yet, the first scheme EUCC (Common Criteria based European candidate cybersecurity scheme) version 1.1. became available in May 2021. ITI also submitted comments to the Cybersecurity Certification Scheme for Cloud Services (EUCS) to provide recommendations such as harmonizing terms and revising prescriptive technical security requirements based on ITI's Cybersecurity Certification Policy Principles. In 2022, ITI expects to see increasing activities to implement the EU Cybersecurity Act including the proposal of new certification schemes, potentially related to 5G security.

EU-U.S. Trade and Technology Council

In September 2021, the United States and EU held the inaugural meetings of the EU-U.S. Trade and Technology Council (TTC). While the preliminary scope of the Council does not envision explicit engagement on cybersecurity policy, there are several venues within the TTC for potential cooperation, including established working groups on technology standards, global trade concerns, ICTS security and competitiveness, and promoting SME access to - and use of - digital tools. In addition, the industry supports the mission of the TTC to grow bilateral technology trade and investment while strengthening global cooperation on digital policy and supply chains. ITI issued a blogpost highlighting areas that the TTC can foster technology and supply chain cooperation, such as establishing a commitment to base regulatory requirements on international standards, taking actions to improve the resilience of semiconductor and other strategic supply chains and ensure export controls alignment, and expanding research and development of trusted 5G infrastructure. In 2022, we hope to see progress from these working groups to identify concrete actions and policy exchange opportunities.

Asia-Pacific

China Cyber Laws and Regulations

Since passage of China's Cybersecurity Law (CSL) in November 2016, implementation measures have been the top priority for the Cyberspace Administration of China (CAC) to fill out the framework prescribed by the CSL. This year, the Chinese government passed the Data Security Law (DSL), the Personal Information Protection Law (PIPL), the Critical Information Infrastructure regulation, and updated Cybersecurity Review Measures. In many cases, these laws and regulations have been in draft for several years. Various iterations of the drafts have incorporated some industry feedback; however, most have not been fully implemented. The Chinese government's recent focus and enforcement on domestic companies has also led to increased attention – and some confusion on compliance-with domestic companies and local authorities working to interpret the overarching laws. In 2022, publications of various regulations are expected to continue strengthening the CSL framework, including a pending catalogue that defines "important data" from the DSL that would inform the implementation and interpretation of the policy trend.

Singapore Cybersecurity Labeling Scheme

For years, the Cybersecurity Agency of Singapore (CSA) has implemented the cybersecurity Labeling Scheme (CLS) for IoT devices as a voluntary scheme. However, this year, the CLS for Wi-Fi routers became mandatory for level 1 in an effort to ensure the quality of security for these devices. The CSA has provided a one-year transition period for implementation, making the scheme fully enforceable in 2022. Required labels are valid for a maximum of 3 years and shall be displayed on both the packaging and the product. The CLS does not currently allow e-labeling as an option and has not yet defined IoT specifically. Further, CLS is based on ETSI standard EN 303 645, and the CSA is interested in exploring collaboration on international adoption. As the recent U.S. Cyber EO specifically referenced Singapore's scheme as a potential starting point for U.S. policy on security labeling, the development of the CLS scheme in 2022 could have significant impact on other global proposals.

Australia Critical Infrastructure

The Australia Ministry of Home Affairs introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to the Parliament, which seeks to amend the Security of Critical Infrastructure Bill of 2018. The amendment seeks to manage the complex security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure, applying to approximately 200 assets in the electricity, gas, water and ports sectors. ITI testified before the Australian Parliament on the Bill, highlighting several concerns with the Bill, including its proposal to allow the government to take control of a critical infrastructure asset, mandatory cyber incident reporting requirements, and inclusion of data storage/processing as a critical infrastructure sector. We expect to see further revisions in 2022, though the timeline for the Bill's passage is unclear.

Australia's Reform of Cyber Security Regulations and Incentives

The Australian Government has launched an effort to establish more comprehensive cybersecurity regulations that simultaneously respond to the growing digital economy, as well as the growing threat of cyber incidents. ITI responded to Australia's *2020 Cybersecurity Strategy Consultation* and was most recently invited to provide feedback on the Government's discussion paper, *Strengthening Australia's Cyber Security Regulations and Incentives*, where ITI shared recommendations on improving the current regulatory environment and governance principles for large businesses. ITI also shared global best practices for standards for smart devices and cybersecurity labeling. The outcome of this consultation session will form part of *Australia's Cyber Security Strategy 2020* and will complement the critical infrastructure reforms and the *Review of the Privacy Act 1988*. The Government is expected to hold additional consultation sessions to shape the national cybersecurity policies, though there have been no announcements regarding future consultations or drafting of regulations.

Americas

Brazil Cybersecurity for Network Equipment

Earlier this year, Act 77 introduced cybersecurity requirements for customer premise equipment (CPE) covering terminal equipment with an Internet connection or equipment of telecommunications networks. ITI submitted comments encouraging the Brazilian National Telecommunications Agency (ANATEL) to retain self-declarations as the conformity assessment method to speed up the implementation of rules, but stay flexible to ensure alignment with international standards and schemes in development and cautioning not to pursue a certification model. However, there are discussions within ANATEL to shift this approach to mandatory cybersecurity requirements, which may expand to all equipment in any circumstances, including IoT devices. In 2022, we expect activities around network equipment cybersecurity to pick up and industry to continue advocating for a flexible, harmonized, risk-based approach to cybersecurity.

Brazil Information Security Requirements for Cloud in the Federal Public Administration

GSI has revoked Ordinance no. 9 of March 2018, and put in place Normative Instruction no. 5 of August 2021, which provides for information security requirements for the use of cloud computing solutions by entities of the Federal Public Administration. There are data localization obligations for information considered classified or confidential. Additional data processed by the Federal Public Administration may be stored abroad, but only in countries previously approved by the Information Security Committee of each entity.

ITI

Promoting Innovation Worldwide

www.itic.org