SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Will the Biden Administration's 'Made in America' Executive Order Present Significant New Cybersecurity Obligations for Transit Operators?

2113-WP
June 2021

Scott F. Belcher, JD, MPP, Harlan Belcher, Katie Seckman, and Brandon Thomas

Cybersecurity threats have become increasingly disruptive to business, government, and consumers. The rising threat was brought into sharp focus in May 2021 when the ransomware attack on the Colonial Pipeline abruptly interrupted business operations and gasoline distribution across the southeast United States. This follows the 2020 SolarWinds and Microsoft server breaches, as well as numerous attacks against public sector entities. The transit industry has not escaped attention from targeted system breaches—the Bay Area Rapid Transit system, the Southeast Pennsylvania Transportation Authority, and Vancouver's Translink are a few of the operators that have recently fallen prey to cyber incidents.

A series of Executive Orders (EOs) and laws over the past several years, including President Biden's EO 14005 Ensuring the Future Is Made in All of America by All of America's Workers seek to centralize the production of key components of the industrial supply chain here in the United States, specifically, key technical hardware.[1] Among the industries and businesses impacted by the EOs are transit providers and their respective vendors. The EOs, although marketed through a patriotic and political lens, address the tangible threat posed to our increasingly hyperconnected lives by a myriad of cyber threats, including ransomware attacks.

Transit operators should expect the heightened focus on supply chain centralization and the need to bolster cyber literacy and protections for the public and private sectors to directly impact their core business and operational considerations, including timely access to affordable product. The need to understand the critical nature of the threats to the transit industry are quickly shifting from good business practices to regulatory compliance.

How Did We Get Here? The Risk Convergence Primer

While the increasing automation and level of connectivity involved in business operations today improves efficiency and service delivery, it has also created an environment prime for exploitation by anyone with the requisite skillsets. Understanding the infrastructure that has permitted individuals, organizations, and nation-states around the globe to disrupt systems thousands of miles away is a critical first step to understanding the application of EOs to businesses and the subsequent actions needed to not only encourage transit operators into compliance but also help them deter and prepare for evolving cyber threats.

Information Technology (IT) vs. Operational Technology (OT)

Information Technology (IT) typically includes the use of computers, networking/physical devices, storage, and infrastructure to create, exchange, and use all forms of electronic data.

Operational Technology (OT) traditionally associated with industrial environments are designed to monitor and manage assets and equipment. Put more simply, OT is the hardware and software that keeps things running.

The rapid development of IT capabilities that includes big data analytics and machine learning/ artificial intelligence has turned OT systems, which were not traditionally networked technologies (i.e., connected to the internet) into well-established points of convergence. This has enabled industries to benefit from innovations in IT that have directly improved controls, maintenance, diagnostics, and reduced business disruptions in OT hardware.

The convergence, however, by virtue of IT's reliance on the internet has expanded cyber risk across what had traditionally remained a siloed OT infrastructure. By increasing the attack surface to operational hardware and equipment, malicious cyber actors can exploit vulnerabilities to disrupt, stop, and/or control industrial hardware. These actors deploy a variety of methods to exploit vulnerabilities to infiltrate an organization's network and gain access. Reducing the opportunity space where such vulnerabilities exist begins with deliberate efforts to improve an organization's cybersecurity posture by evolving the ecosystem of people, processes, and technologies aimed at managing cyber risk.

Virtual cyberattacks based on security or software flaws are certainly common, but the easiest path for a malicious cyber actor to follow is gaining physical access to a desired system. Executive Order 14005, also known as 'Made in America,' acknowledges this significant risk and mandates greater scrutiny of the origin of hardware and its associated supply chain. A hostile nation or other nefarious actor, for example, could easily partner with a local manufacturer to create a sophisticated "back-door" in a product destined for consumption in the United States. Either as a stand-alone product or integrated with other hardware, once it is connected to the internet, the bad actor could exploit the hidden "back-door" to their advantage and at their leisure inflict significant damage before it is discovered and remediated.

'Made in America' Executive Order

In January 2021, President Biden signed EO 14005 with the stated goal of strengthening federal laws that require government agencies to give preference to U.S. firms in federal procurement, federal grants, and other forms of federal assistance. The EO directs the Federal Acquisition Regulatory Council and the Office of Management and Budget to take multiple actions, including increasing domestic content requirements for a product to qualify as a domestic good and increasing the stringency with which the new rules are enforced. Requests for waivers will now be centrally reviewed and published online, increasing transparency of the process and of the companies seeking exception to the rule. Based on the stated goals of the other EOs highlighted in this report, information and communications technologies are unlikely to be considered for 'Made in America' waivers.

Executive Orders Target Global Supply Chains

Prior to the 'Made in America' EO, the Trump Administration issued EO 13873, *Securing the Information Communications Technology and Services Supply Chain*, in May 2019, which acknowledged the critical nature of information and communications technology services (ICTS) and how ubiquitous they are in support of critical infrastructure.[2] The interim final rule from the U.S. Department of Commerce went into effect in March 2021.[3] The relatively broad scope of the EO's application to technologies and products and the broad application of the term "foreign adversary" in this application means that multiple components of a transit operator's system—including some software, hardware, and cloud or network services—now fall under this regulation.

In December 2019, the Trump Administration signed into law the National Defense Authorization Act (NDAA) for Fiscal Year 2020, which included a provision banning the use of federal funds to purchase "rolling stock" (e.g., cars, vans, buses, and rail cars) for use in public transportation made by companies owned, controlled, or otherwise affiliated with a country identified by the U.S. Trade Representative on its Priority Watch List, including China.[4] This will have direct implications for the procurement of electric transit buses from Chinese bus manufacturer BYD, which has the most electric buses in operation in the United States and has been the largest electric bus manufacturer in the United Stated for the past three years. Although the Office of the United States Trade Representative's Priority Watch List is subject to regular political review, we are unlikely to see a thaw in trade relations with China before the law goes into effect on December 20, 2021.

The Exception to NDAA's "Rolling Stock" Ban

The 2020 NDAA directed U.S. transit agencies not to purchase buses made in China using federal funds; however, a two-year phase-in period for the "rolling stock" ban gives transit agencies the ability to continue to execute contracts for these vehicles without exception.[5] The Federal Transit Administration (FTA) has clarified that if an FTA grant recipient executes a contract on or before December 20, 2021, that contract will be eligible for grant funding even if the delivery of vehicles occurs after the law's effective date. This explains why Washington state, various Massachusetts transit agencies, and others have successfully executed contracts with bus-maker BYD in 2021. They face no penalties for doing so under the current law.

The FTA has further clarified that if a base contract is entered into prior to December 20, 2021, based on the recipient's reasonably foreseeable vehicle needs, future options up to five years after the date of contract execution will be honored.

In response to persistent Russian cyberattacks and other acts of aggression directed at the United States and its allies, President Biden issued EO 14024, *Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation*, in April 2021, implementing new sanctions on Russian entities, including technology companies known to have ties to the Russian Intelligence Services.[6] Given the services these companies render to their government clients, some of them are likely to have contributed to Russia's SolarWinds cyberattack, which threatened U.S. national security and public safety.

One week after the Colonial Pipeline ransomware attack, on May 12, 2021, the Biden Administration released Executive Order 14028, Improving the Nation's Cybersecurity, further underscoring the U.S. government's acknowledgement that the United States needs to take additional action to secure our digital infrastructure and that they are looking to the private sector as partners in this process.[7] The EO calls on private sector companies to make the necessary cybersecurity investments to help prevent and deter cyberattacks and improve threat reporting to the federal government. The primary focus of the EO is on improving the government's preparedness for and response to cyber incidents—including new cybersecurity requirements for government contractors. The nature and the scope of work proposed in the text is ambitious but vague, so organizations are advised to familiarize themselves with the EO and watch for a succession of proposed actions across federal agencies, which are likely to influence agency expectations for their non-government partners.

Implications for U.S. Transit Operators

Restricting the supply chains of major transit providers across the United States does not replace the need for more stringent cybersecurity mechanisms across the industry (see the Mineta Transportation Institute (MTI) study on transit cybersecurity, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, for more details).[8] The targeted supply chain actions should, however, prompt transit operators to consider if and how they will prepare for and, in some cases, quickly comply with increasingly stringent rules. Even in instances where exceptions are being made to accommodate transit agencies purchasing needs, these agencies need to be aware of the associated cyber risks and, ideally, account for the risk in their cyber contingency plans.

First Steps toward Cyber Maturity

The Washington Metropolitan Area Transit Authority (WMATA) is in the process of building a robust Supply Chain Cybersecurity Program. Though still in its developmental phase, the program has matured substantially over the last year, spurred on by increased government scrutiny of suppliers, most notably those in China. WMATA's program operates on the premise that all procured information and operation technology is inherently at risk, regardless of where it is manufactured. The WMATA program includes a cybersecurity professional as an approver in all procurements involving technology. This can be a challenge, as technology is often incorporated into solicitations where a person may not expect to find it (e.g., construction of a new rail station). Closed circuit television (CCTV) cameras, elevators or escalators, and information displays should all be considered IT-related procurements.

Key Considerations for Public Transit Operators and Their Suppliers

- The supply chain restrictions in multiple Executive Orders suggest that U.S. transit agencies will likely need to find new sources for multiple products, including items purchased from or containing components produced by Huawei and other Chinese providers.

- More sourcing limitations are likely to reduce the number of acceptable vendors, potentially increasing the cost of goods. Removing Huawei—the largest telecommunications product provider in the world and one of the largest chip manufacturers,—for example, will

reverberate up and down the supply chain, increasing the need for operators to have line of sight to multiple layers of their supply chain.

- Transportation executives should educate themselves about the exemption processes associated with each of the EOs, the government agency staff leading the efforts (they are a good resource for EO interpretation or clarification), and, when needed, take action to file an exemption request. Doing so may only provide temporary relief to sourcing concerns but could give transit operators the time they need to identify or develop new vendor relationships.

- The 'Made in America' EO and similar directives demonstrate a level of consistency in U.S. policy across party lines. In short, future policies aimed at making the U.S. supply chain more resilient and creating more American jobs in the process are unlikely to deviate much from the current playbook. Waiting for political change is unlikely to address the need to invest in order to comply with new regulations.

The transportation infrastructure is a prime target for nefarious actors seeking to disrupt communities, be it for personal or political gain. The avenues to exploit this vital infrastructure will continue to evolve with the technology that enables the industry's core operations and goals. Accounting for the risk today will foster greater resiliency and preparedness in the years to come.

Endnotes

1. https://www.federalregister.gov/documents/2021/01/28/2021-02038/ensuring-the-future-is-made-in-all-of-america-by-all-of-americas-workers

2. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

3. https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

4. https://www.congress.gov/bill/116th-congress/senate-bill/1790

5. https://www.transit.dot.gov/funding/procurement/frequently-asked-questions-regarding-section-7613-national-defense

6. https://www.federalregister.gov/documents/2021/04/19/2021-08098/blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the

7. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

8. https://transweb.sjsu.edu/research/1939-Transit-Industry-Cyber-Preparedness

Acknowledgements

The authors thank MTI staff, including Executive Director Karen Philbrick, PhD; Deputy Executive Director Hilary Nixon, PhD; Graphic Designer Alverina Eka Weinardy; and Communications and Operations Manager Irma Garcia.

About the Authors

Scott Belcher, JD, MPP, is the CEO of SFB Consulting, LLC. Prior to founding SFB Consulting, LLC he served for two years as the CEO of the Telecommunications Industry Association and for seven years as the CEO of the Intelligent Transportation Society of America. Kathryn Seckman is a geopolitical risk and strategy professional, specializing in bringing the best practices of the intel sector to global business. She is a Fulbright Scholar, holds an MA in Security Studies from Georgetown University, and a BA in International Relations from Drake University. Harlan Belcher is a Master of Environmental Management student concentrating on Energy at Duke University's Nicholas School of the Environment. Before pursuing his Masters he worked as a wildland firefighter in Northern California for several years. Brandon Thomas is a Partner at Grayline Group, a firm focused on helping organizations understand and manage for disruption, as well as a Managing Partner of Blockview Partners, a firm focused on understanding the emerging blockchain and cryptocurrency space.

This report can be accessed at transweb.sjsu.edu/2113WP

MTI is a University Transportation Center sponsored by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology and by Caltrans. The Institute is located within San José State University's Lucas Graduate School of Business.