September 2020

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

QUENTIN E. HODGSON, MARYGAIL K. BRAUNER, EDWARD W. CHAN

Securing U.S. Elections Against Cyber Threats

Considerations for Supply Chain Risk Management

On January 9, 2020, the U.S. House of Representatives Committee on House Administration heard testimony from the chief executive officers of Election Systems and Software (ES&S), Hart InterCivic, and Dominion Voting Systems, the three largest vendors of U.S. election equipment.[1] The committee chair asked each of the three leaders whether their companies' equipment contained components from either Russia or China, basing her question on a recent Interos report that stated that 20 percent of the components in one major election equipment vendor's machine came from China.[2] All three executives noted that they use Chinese-manufactured components in their election equipment, in part because they did not have viable domestic sources for these components.[3] The hearing reflects a broader concern about the exposure that technology supply chains have to China, combined with a widening focus on election security in the United States that gained prominence following Russian interference in the 2016 elections but has extended to encompass many worries about foreign actors' ability to interfere with a core component of American democracy.

In January 2017, then–Secretary of Homeland Security Jeh Johnson declared election infrastructure to be part of the nation's critical infrastructure, designating it a subsector of the Government Facilities critical infrastructure sector.[4] Since that designation, the federal government, through the Cybersecurity and Infrastructure Security Agency (CISA), has placed significant emphasis on election system cybersecurity, reaching out to state and local election officials around the country to offer cybersecurity services and advice. As part of that work, CISA convened two advisory councils, one of government officials from the federal, state, and local levels in a government coordinating council (GCC) and the other drawing from the election system vendor community in a sector coordinating council (SCC). The initial Election Infrastructure Subsector-Specific Plan approved in 2018 called for the GCC to "partner with the SCC to facilitate election security improvements across the election supply chain."[5] This initiative prompts questions on what improving security in the election supply chain entails and how DHS and others can work with both the vendor community and election officials to achieve this objective.

This Perspective focuses on the cybersecurity risk to election supply chains. We start with a brief discussion of election infrastructure and the stakeholders involved. We then examine what cyber supply chain risk management (SCRM) means in the context of U.S. election systems. Finally, we explore how traditional frameworks for SCRM can be adapted to meet the needs of the election community in the United States.

It is important to note that SCRM is only one of several issues that the United States faces in securing its elections. As many analysts have noted elsewhere, disinformation campaigns, mail fraud, and cyber threats to election systems are very real and potentially more-likely threats than supply chain

Abbreviations

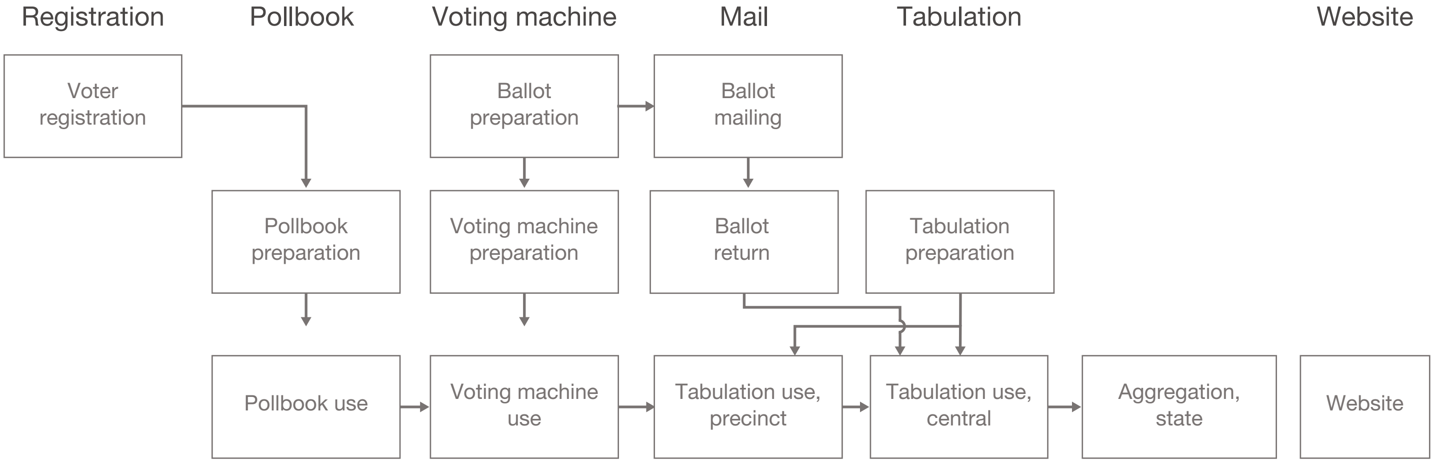
BOKN	Business Open Knowledge Network
CISA	Cybersecurity and Infrastructure Security Agency
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
EAC	U.S. Election Assistance Commission
ERIC	Electronic Registration Information Center
ES&S	Election Systems and Software
GCC	government coordinating council
HAVA	Help America Vote Act of 2002
ICT	information and communication technology
IR	interagency or internal report
NIST	National Institute of Standards and Technology
PII	personally identifiable information
SCC	sector coordinating council
SCRM	supply chain risk management
SP	special publication

concerns are.[6] But, as we explore in this Perspective, the potential for scaling attacks to affect a broad swath of the American election landscape makes the supply chain an attractive avenue for adversaries and therefore cannot be ignored.

SCRM is a broad discipline that addresses a variety of potential risks, such as disruptions stemming from natural disasters, political upheaval, or public health emergencies, such as coronavirus disease 2019 (COVID-19). This Perspective focuses on the deliberate targeting of election system supply chains through cyber means. We do not address other supply chain disruptions, such as the inability to get raw materials, parts, or components in a timely fashion. These are things that would affect a manufacturer's ability to make election equipment and, therefore, a jurisdiction's ability to buy election equipment. This is an additional concern for election officials, particularly as they plan for the 2020 general election and beyond in the face of potential continued effects caused by the COVID-19 pandemic.[7]

To understand how cyber SCRM applies to election systems, we start with a look at the election system's cyber infrastructure. An election system is really a series of computers and digital and analog components each performing specific tasks that may be networked together while in use or when programmed. Figure 1 provides an overview of a generic election system, highlighting the system components and interactions across components.

FIGURE 1
Components of an Election System



The start of the process is voter registration, which involves creating, populating, and maintaining a database of records of eligible voters. Voter registration information is used to populate pollbooks for verifying each voter at a polling center or precinct and providing them with the correct ballot. In preparation for an election, ballots and voting machines are prepared by laying out contests using software and programming voting machines. During an election, voters may use voting machines of various types (e.g., ballot-marking devices for paper ballots, direct-recording electronic machines that record choices directly to digital media). Paper ballots are scanned using high-speed scanners. Then, ballots are tabulated and results reported through formal election night reporting channels, as well as through postings of results on websites.

Stakeholders in Election Security

Although every voter has a stake in and should be concerned about election security, the role of the voter is primarily to voice their concerns to election officials, policymakers, and elected leaders. In this section, we briefly review the roles of the other primary stakeholders in election cyber SCRM. We discuss the considerations that inform their responsibilities and how they interact with other stakeholders. We address state and local election officials,[8] federal stakeholders, vendors of election system equipment and services, and researchers and advocacy groups.

State and Local Officials

The U.S. Constitution makes each state responsible for establishing the times, places, and manner in which it chooses representatives and senators,[9] as well as how it appoints electors for choosing the president and vice president.[10] As a practical matter, this has led to each state establishing its own structures and processes for overseeing elections, including the degree of centralization or devolution, the types of technology to use, and what forms of voting are allowed (e.g., early voting, vote by mail). This puts state and local legislatures, elected officials, and election officials at the center of decisions about what equipment to purchase and how to implement election infrastructure. Given the diversity in size and resources, state and local officials also have varying levels of influence over the supply chain in terms of purchasing power and regulatory roles. For example, although California is the largest U.S. state by population, it also devolves significant authority to its local jurisdictions and therefore does not speak with one voice to the vendor community.[11] Georgia, on the other hand, has centralized governance at the state level, including equipment purchases, which allows the state to negotiate with vendors with a single voice. Election officials do not make these choices unilaterally. However, they must justify budgets; work with other parts of state and local government; and engage state governors, legislatures, and county boards on legislation and budgets.

Federal Officials

At the federal level, the principal stakeholders involved in assisting state and local governments to secure their election systems are CISA, the U.S. Election Assistance Commission (EAC), and the National Institute of Standards and Technology (NIST). These are the principal players, although others play supporting roles (e.g., the Federal Bureau of Investigation, which is charged with investigating cyber threats from criminals, overseas adversaries, and terrorists; the intelligence community, which provides intelligence and analysis on adversary activities).

CISA is the principal operational component in DHS that is responsible for working with critical infrastructure sectors to assess risk and support activities to secure them from cyber and physical threats. Its mission is to "[l]ead the National effort to understand and manage cyber and physical risk to our critical infrastructure."[12] Since the 2017 designation of election infrastructure as a subsector of the Government Facilities sector, CISA has been working with the election community to improve cybersecurity, including convening and co-chairing the Election Infrastructure Subsector GCC and SCC, as noted previously, as well as creating the Elections Infrastructure Information Sharing and Analysis Center at the Center for Internet Security.[13]

EAC, an independent, bipartisan commission established with the passage of the 2002 Help America Vote Act (HAVA),[14] develops guidance to meet HAVA requirements, creates voluntary guidelines for voting systems, shares information on election administration, accredits testing laboratories, and certifies voting systems.[15]

NIST issues guidance and develops cybersecurity standards. NIST manages the National Software Reference Library, which is a repository of software that allows organizations to check their installed software against the versions in the library for any unauthorized changes.[16] HAVA also charged NIST with helping EAC develop the voluntary voting system guidelines.[17]

Vendor Community

As we noted at the beginning of this Perspective, there are three main election system vendors in the United States, but they are not the only players in the market. The membership of the DHS-convened Election Infrastructure Subsector SCC indicates the breadth of stakeholders in the private sector. The 28 member companies and organizations are shown in Box 1.[18]

Most of the SCC members are companies that provide hardware, software, or services related to

BOX 1

Members of the Election Infrastructure Subsector Sector Coordinating Council

- Amazon Web Services
- Arikkan and Chaves Consulting
- Associated Press Elections
- BPro
- Clear Ballot
- Crosscheck
- Democracy Live
- Democracy Works
- Demtech Voting Solutions
- Dominion Voting Systems
- ES&S
- Electronic Registration Information Center (ERIC)
- Hart InterCivic
- KNOWiNK
- Microsoft's Defending Democracy Program
- MicroVote General Corporation
- NTS Data Services
- PCC Technology
- Pro V&V
- Runbeck Election Services
- Scytl
- SLI Compliance
- Smartmatic
- Tenex Software Solutions
- Unisyn Voting Solutions
- VOTEC
- Votem
- VR Systems

conducting elections; they include the three major election equipment manufacturers, the largest cloud service provider, and small businesses focusing on certain segments of the marketplace or election infrastructure. Two of the members, Pro V&V and SLI Compliance, conduct system testing. The Associated Press news organization, which provides election polling and reporting on election returns for every jurisdiction in the country, and ERIC, a nonprofit organization that facilitates validation of state voter registration information, are also members.

Researchers and Advocacy Groups

Finally, and no less important, are researchers and advocacy groups that seek to inform the public about election issues across the political spectrum. Advocacy groups include a wide array of organizations that focus on such issues as voter access, fraud, and promoting election reform. Researchers identify potential cyber risks in systems and conduct analysis on their implications for voting system integrity and access.

For example, the organizers of DEF CON, the largest annual hacker conference, have a section—the Voting Machine Hacking Village, also known as the Voting Village—devoted to allowing participants to test (i.e., attempt to break into) voting machines and other election equipment that the organizers have procured on the open market. In addition to identifying vulnerabilities in specific pieces of equipment, the event seeks to more generally raise awareness of the cybersecurity risks associated with election systems. From the Voting Village organizers' perspective, its work in exposing security flaws is meant to ultimately make voting more secure:

> The clear conclusion of the Voting Village in 2019 is that independent security experts and hackers are stepping into the breach—providing expertise, answers, and solutions to election administrators, policymakers, and ordinary citizens where few others can.[19]

Members of the election community who criticize the Voting Village include vendors who state that the conditions in which the testing occurs are not realistic and election officials who are concerned that the publicity associated with successful but (in their view) unrealistic attacks can lead to voters questioning the integrity of elections.[20] To promote more collaboration between election officials and the cybersecurity community, CISA has issued a guide for establishing a vulnerability disclosure program.[21]

The Risk to Election Supply Chains

The types of cyber attacks that worry election officials are, broadly speaking, those that provide adversaries the ability to

- exfiltrate confidential data at scale (i.e., **confidentiality attacks**), although this may be less impactful on the running of elections[22]
- attack election integrity by manipulating results (i.e., **integrity attacks**)
- interfere with the smooth running of elections by denying the use of equipment at critical moments (i.e., **availability attacks**).

Much of the focus on election security has been at the jurisdiction level.[23] However, jurisdictions are not the only places where systems can be attacked. Voting machines and other election equipment could be attacked before they ever come into a jurisdiction's possession by attacking somewhere along the jurisdiction's supply chain—the path that the

Stakeholders must defend three especially crucial aspects of U.S. elections: confidentiality, integrity, and availability.

components take on their way from being parts to becoming a finished product delivered to the election jurisdiction.

A supply chain attack's main attraction to an adversary is its potential for a greater scale of impact than would be possible through other means. The U.S. election system, unlike systems in many other countries, is diverse in terms of technology, people, and governance. Elections are administered and run at the state and local levels, with a limited federal role. Each state determines how much it will centralize that administration or devolve it to local jurisdictions. Election systems are not normally connected across state boundaries, with the exception of the ERIC system, which facilitates voter registration record deconfliction, currently used by 30 states and the District of Columbia.[24] Voting machines, for example, can be highly localized, with some jurisdictions purchasing their own systems separately from the state. Kentucky is one example of this, whereas Georgia and Delaware are much more centralized in approach.[25] However, an attack on the voting machine supply chain would have the potential to compromise multiple jurisdictions throughout the country.

Consider this example of voting machines and supply chain risk: In the United States, 59 types of voting machines are available to the more than 240 million registered voters.[26] In terms of production of units, 47 percent are manufactured by ES&S, 29 percent by Dominion, and 14 percent by Hart InterCivic.[27] Together, these three companies make 35 of the 59 types of machines in use and account for 90 percent of the units.[28] Furthermore, because voting machines are essentially computers that need to perform only a limited set of simple functions, it is likely that many of the machines have parts made by the same suppliers. The extent of common parts is illustrated by the dominance of Intel central processing units, with 93-percent market share for server processors.[29] Thus, attacking a relatively small number of suppliers could compromise a large percentage of voting machines.

A large-scale supply chain attack on an election equipment manufacturer could allow an adversary to prestage functionality on a logic board in a voting machine to execute an attack either with specific intention, such as altering votes in a specific way, or in a randomized way to sow confusion. Such an attack would be difficult, if not impossible, to detect ahead of time, given the difficulty of identifying components that have been altered.[30]

In 2018, *Bloomberg Businessweek* published an exposé that asserted that a Chinese manufacturer inserted chips on the motherboards it sold to large U.S. corporations to allow hackers to infiltrate the corporations' networks.[31] The allegations in the article are contested, and most U.S manufacturers are reluctant to make public any cybersecurity breaches.[32] Yet experts are concerned because security researchers have demonstrated the ability to implant hardware that could cause malicious damage or enable unauthorized access while escaping detection. At the 2018 SANS Industrial Control Systems Europe Summit, for example, cybersecurity researcher Monta Elkins demonstrated such an attack.[33]

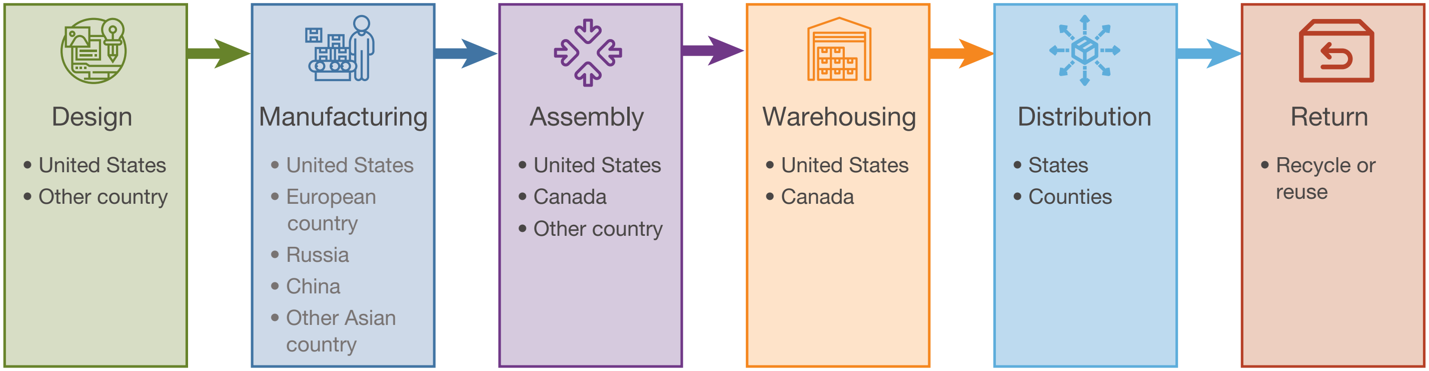
The supply chain is an ecosystem that can change over time. Figure 2 diagrams a supply chain and includes the following phases, at any of which an attack can occur: (1) design, (2) manufacturing of components, (3) assembly, (4) warehousing, (5) distribution, and (6) return. The Interos report cited during the House hearing asserts that 59 percent of the companies in the first three tiers of the supply chain for the company examined had locations in China, Russia, or both.[34] Although having a business location in either country would not in itself mean that components going into election equipment would be compromised, but the ties to those countries raised concerns in Congress.[35]

A cyber supply chain attack can occur at any point in the supply chain:

- **Design:** The equipment may have an intentionally vulnerable product design.
- **Manufacturing:** During the manufacture of hardware, malicious chips or exploitability can be added to motherboards or other components. Similarly, software and firmware can be modified in difficult-to-detect ways.
- **Assembly:** Like in manufacturing, malicious chips or other components can be introduced into products.
- **Warehousing:** Adversaries can introduce malicious components into products before

FIGURE 2

Phases and Participants in a Supply Chain for Election Equipment for Use in the United States



SOURCE: The countries listed are found in Interos, 2019.

they are shipped to intermediate distribution hubs or end customers.

- **Distribution:** Products can be intercepted during distribution to introduce malicious components or otherwise alter the functionality of hardware or software.
- **Return:** Election equipment can be purchased in an electronics resale market, such as online through eBay and other web markets. Even if such equipment is not purchased for use in an election, the availability of resale equipment provides malicious actors an opportunity to identify vulnerabilities, develop counterfeit components, and plan attacks. There is the risk that election machines may not be "wiped clean" of data prior to disposal, thus increasing the risk of compromising personal and election information.[36]

Approaches to Supply Chain Risk Management

SCRM originated in the business world, in which the primary initial focus was on addressing the risk of volatility in supply chains for manufacturing processes. As companies outsourced the manufacture of more components, particularly to overseas locations, they had to contend with a variety of factors that could interrupt the flow of components, from weather conditions to political instability or economic factors.[37] Supply chain experts also had to contend with potential counterfeit parts, such as electronic components that did not perform to standard or could pose a safety hazard, making their way into systems.

Cyber SCRM, on the other hand, is of more-recent vintage. NIST began its focus on information and communication technology (ICT) SCRM in 2008 as part of the George W. Bush administration's Comprehensive National Cybersecurity Initiative.[38] The ICT SCRM program at NIST led to, among other things, the development of a NIST special publication (SP) on SCRM for federal information systems.[39] DHS convened its own ICT SCRM task force in October 2018, drawing on membership from major technology companies (e.g., Samsung, Cisco), telecommunication companies (e.g., AT&T, CenturyLink), and cybersecurity firms (e.g., Palo Alto Networks, FireEye).[40] In March 2020, NIST issued an impact analysis tool to help map interdependencies in cyber supply chains.[41] These efforts are not focused specifically on election infrastructure but do point to a growing federal focus on cyber SCRM more broadly. Box 2 summarizes the four approaches, detailed in this section.

Cybersecurity and Infrastructure Security Agency Supply Chain Risk Management Essentials

In May 2020, CISA published *SCRM Essentials* to recommend actions that organizations, managers, and staff can take to manage supply chain risk.[42] CISA developed the guide using related key practices and guidance in *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.*[43] With some modification, these actions are applicable to the election supply chain. For example, the election supply chain does not have a financial "bottom line" to protect like commercial supply chains do, but it does have an equivalent in the form of "public trust": A functioning democracy depends on the public's perception of an election's integrity. The CISA guide is designed for companies and shows actions that leaders and staff should take. Rather than identifying actions for solely one company, addressing risks in the election supply chain must also identify actions to be taken at the federal, state, and county (local) levels. These actions must be coordinated and integrated across those levels.

The six essential steps in *SCRM Essentials* are as follows:

1. **Identify:** Determine who from the organization needs to be involved.
2. **Manage:** Develop supply chain security policies and procedures.
3. **Assess:** Understand the hardware, software, and services being procured.
4. **Know:** Map the supply chain to better understand what components are procured.
5. **Verify:** Determine how the organization will assess the security culture of suppliers.
6. **Evaluate:** Establish systems for checking supply chain practices against guidelines.

Appendix A, later in this Perspective, provides a matrix for election officials and other stakeholders to use; the SCRM steps are the rows and the elements of the supply chain are the columns.

A functioning democracy depends on the public's perception of an election's integrity.

BOX 2

Four Approaches to Cyber Supply Chain Risk Management for Election Equipment

- CISA specifies six steps for entities throughout the supply chain to take:
  (1) Identify who needs to be involved.
  (2) Develop security policies and procedures.
  (3) Assess what is being procured.
  (4) Map the supply chain for those procurements.
  (5) Set up verification for suppliers' security.
  (6) Establish a way to evaluate practices.
- EAC tests and certifies election systems.
- DoD sets requirements for contractors to protect their supply chains.
- NIST develops guidance and tools for entities to implement to assess and improve their security processes.

These actions are shown at the federal, state, and county levels. To use the matrix for the first step (identify), the person completing the matrix would create a separate list of people for voter registration, pollbook, voting machine, scanners, and tabulation. There is likely an overlap of the same people performing several of these tasks. Because it is likely that the people involved in elections will change over time, every row of the matrix should be reviewed frequently.

Election Assistance Commission Testing and Certification

An important part of current efforts to mitigate election cyber supply chain risk is the testing and certification of election systems. HAVA specifically states, "The Commission shall provide for the certification, de-certification and re-certification of voting system hardware and software by accredited laboratories."[44] The EAC *Testing and Certification Program Manual* lays out detailed requirements, but participation in the certification process is voluntary.[45] Still, the three main election system vendors highlight their certifications; as one example, the Hart InterCivic website states,

> whereby Hart provides all source code for every component of the voting system, and the code undergoes careful review by test laboratories accredited by both the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP).[46]

Some researchers have questioned the depth of the EAC certification process and the lab tests performed on election equipment; for example, Matthew Bernhard, a software engineer with VotingWorks, points out that certification officials are "not doing X-rays of the motherboards of the machines [to look for malicious chips]. They're just doing some cursory looks at the machines."[47] Whether X-rays ought to be the standard is an open question. But this serves to highlight a larger question of whether current standards are sufficient. There are no requirements for manufacturers to document oversight of contractors who work with their equipment to ensure that security standards for election equipment are met. Additionally, EAC does not require states to certify their election equipment, although many states do. Some local polling sites allow workers to use off-the-shelf laptops and tablets during the election process.[48] There is also a question of when the equipment certification takes place. Currently, EAC certification occurs after the equipment is manufactured but before it is delivered to a customer.[49] As shown in Figure 2, that is very far down the supply chain after design, manufacturing, and assembly. Additionally, the EAC certification does not involve identification of suppliers providing parts and software for the election equipment.

Department of Defense Contractor Compliance Requirements

In the absence of EAC standards on suppliers providing parts and software to election equipment manufacturers, what standard should be applied? Ultimately, election systems are computers, so managing the risk in the supply chain for election equipment should be the same as the way risk is managed for other computer supply chains. The U.S. Department of Defense (DoD) requires strict supply chain security standards and supplier certification.[50] All tier 1 (parts) suppliers must assess and report the compliance of their suppliers to the DoD security standards. The Brennan Center for Justice has recommended that EAC develop similar requirements for suppliers for election system manufacturers. These requirements would include background checks, identification of foreign ownership, and cyber incident reporting.[51]

It could be argued that such requirements would be too onerous for the companies supplying U.S. voting equipment. ES&S, Hart InterCivic, and Dominion Voting Systems have annual sales revenues of $115 million, $39 million, and $47 million, respectively.[52] These are small companies compared with large defense contractors. For comparison, Boeing had $76 billion in revenue in 2019, and Lockheed Martin had sales of $59 billion in 2019.[53] Yet all of these companies have supply chains that look like the one in Figure 2, with design, manufacturing, assembly, and warehousing in both the United States and other countries. Because of DoD requirements, every defense contractor must protect its supply chain from cyber attacks and its products from malware.

The DHS-led ICT SCRM task force identified "[d]eveloping a common framework for the bi-directional sharing of supply chain risk information between government and industry" as its first workstream.[54] To the extent that there are common suppliers for election computer equipment, a supplier's certification or lack thereof could be made available to all buyers of the equipment. DHS's 2017 binding operational directive prohibiting use of any Kaspersky Lab products on federal information systems is an example of a warning about an untrusted supplier.[55] Similar information should be provided about certified suppliers, while noting that certification is a continuous process and certification can be revoked. Because cyber SCRM is a developing field, the frequency of recertification has rarely been addressed; every time there is a design change or sub-tier supplier change or a software update, should there be a recertification? EAC could fund supplier certification just like it funds equipment certification, and it could help establish bidirectional sharing of information.

As of April 2020, 76 suppliers were accredited to provide trusted supply chain products to DoD and the federal government.[56] Currently, the suppliers of election systems are not among these companies, but they could be. Election equipment purchasers across the states could band together or work through EAC to accredit those suppliers or switch to ones that are already accredited. This recommendation can be incorporated into EAC's voting system guidelines. Additionally, states can learn about the compliance or noncompliance of voting systems.[57]

EAC's voluntary voting system guidelines were last updated in 2015 and do not address SCRM.[58] Yet, SCRM is a rapidly evolving field for commercial and government institutions. Many of the NIST and DoD policies and instructions related to SCRM have recently been updated or are in the process of being updated.

National Institute of Standards and Technology Assessment Tools

Although EAC has a self-assessment tool to assist in implementing election security best practices, it does not have a tool for assessing and implementing best practices in the election supply chain. Such tools and guidance are under development, and their adoption in government and the private sector is not universal. Four of the most recent ones are

- "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" (NIST SP 800-161), April 2015.[59] SP 800-161 is a guide for federal agencies on SCRM for their technologies. The guidance is for so-called "high-impact" systems, but, because of interdependencies of systems and components, the guidance might also be useful at lower-impact levels. The publication notes that caution is advised when applying SCRM controls because of the additional costs to suppliers, integrators, and personnel.[60]
- *NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements* (NIST Handbook 162), November 2017.[61] NIST Handbook 162 is primarily a guide for manufacturers supplying equipment to DoD and identifies who must certify that their supply chains comply with the security and cyber incident reporting requirements in Defense Federal Acquisition Regulation Supplement Clause 252.204-7012. In its 2015 and 2019 industry case studies, NIST included many of the suppliers that must meet these requirements. The cyber SCRM key practices from these case studies are summarized in the third publication.
- *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (draft NIST Interagency or Internal Report [IR] 8276), February 2020.[62] The draft NIST IR 8276 highlights practices collected from a series of interviews with industry practitioners and developing case studies. It defines

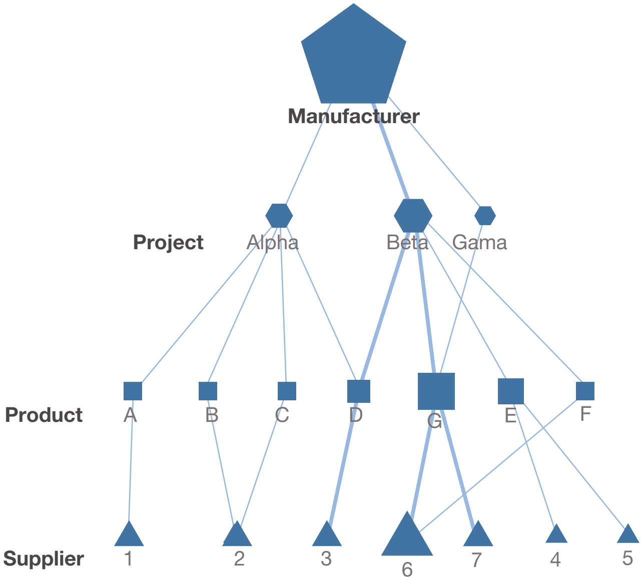
SCRM concepts and maps them to key practice areas.

- *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* (NIST IR 8272), March 2020.[63] In addition to mitigating risk from individual suppliers, manufacturers must assess the interdependencies of their supply chain's products and suppliers with other supply chains using some of the same suppliers. *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* is a draft tool that can give manufacturers insights into which nodes in their supply chains are most critical and the dependencies among their suppliers. The tool gives organizations a visual way to evaluate relative impacts of potential supply chain risks and should be used in conjunction with other risk management tools. For example, an organization should examine inputs to a node that has high impact and interdependence for threat, vulnerability, and likelihood of cyber supply chain risk. Figure 3 displays an example of the kind of hierarchical visualization the tool produces. Presenting the analysis in this form provides a visual cue to where a customer might wish to focus attention or potentially seek to diversify the supply chain to reduce reliance on one supplier (if an alternative is available). This is a new tool, still in draft form, and likely will change based on public comments and as users provide feedback to NIST.

These publications contain key information for industries that must protect their supply chains. Applying the guidance that these publications provide requires resources that are not available in most election organizations, even at the state level. Recognizing this problem, CISA provides advisers, at no cost to the customer, to conduct assessments of

FIGURE 3

An Impact Analysis Tool Visualization



SOURCE: NIST IR 8272 (Paulsen et al., 2020, p. 24).

NOTE: The top node is the company whose supply chain is graphed. The sizes of the triangles, squares and circles can represent dollar value, quantity, or impact. The sizes of the node and lines show the interdependence: Larger nodes have higher interdependence scores (are more interdependent), as do heavier lines.

network security, service providers, and equipment suppliers. The assessments can include pollbooks, voting machines, scanners, and tabulators. U.S. Government Accountability Office researchers on election security found that the biggest challenge for state officials is to find time in the election calendar for scheduling CISA services.[64] To address this challenge, CISA administrators offer remote penetration services to test risk and vulnerability. CISA has also partnered with cybersecurity intelligence firms to conduct webinars for state and local officials.

Such partnering is critical for SCRM. SCRM cuts across all sectors of the government and industry. All of these organizations use computers; all have supply chains that are sourced worldwide and are interdependent; and all are vulnerable to cyber attacks. By collectively vetting suppliers and reporting weaknesses in technology or software, they will reduce the risk that a weakness will be exploited and cause harm.

Business Open Knowledge Network

As discussed in the previous section, partnering is critical to SCRM because supply chains are interdependent. The extent of the interdependence of supply chains is illustrated by knowledge graphs developed by the Business Open Knowledge Network (BOKN) project, an open-source collaboration of computer scientists and business school faculty from several universities designed to provide data and visualizations on business networks.[65] The data in the BOKN project database have been gleaned from many sources (business, manufacturing, and finance) using innovative data science techniques. Figure 4 is an example of a BOKN knowledge graph showing the relationship between companies and suppliers.[66] This particular graph features 3M Corporation, a multinational conglomerate headquartered in Minnesota. The graph reveals both the interdependence of suppliers and the many different countries supplying products to 3M.

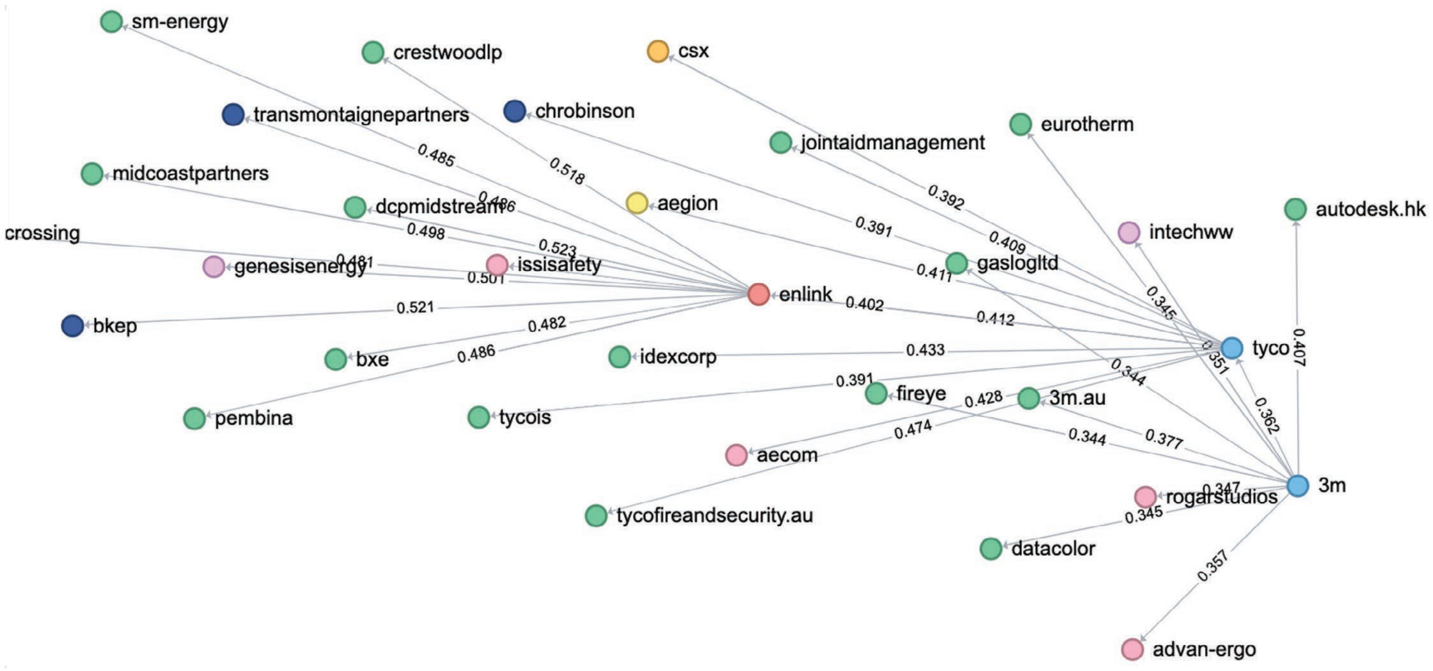
The existence of these graphs, as the project develops them in its ongoing efforts, showing these relationships might incentivize suppliers to become trusted supply chain providers to not only DoD and federal government but all U.S. industry. The information will also help the industry and government know their dependence on suppliers with this certification versus those who do not. Additionally, the knowledge graphs illustrate the importance of cyber incident reporting because the vulnerabilities and their spread can be traced through many overlapping supply chains.

Impact Analysis Tool for Interdependent Cyber Supply Chain Risks

In the publication *Cyber Security in Elections: Models of Interagency Collaboration*, the authors state that “scrutiny and careful selection of trusted

FIGURE 4

Knowledge Graph Showing Relationships Between Companies and Suppliers



SOURCE: Information Sciences Institute, 2020, p. 46. Used with permission.

suppliers and vendors" are critical mitigation measures.[67] As previously discussed, the trusted supplier program is an important tool for DoD efforts to ensure trusted suppliers for microelectronic parts in defense systems. We recommend incorporating it into the process of ensuring that suppliers of election equipment pass similar standards. The U.S. Cyberspace Solarium Commission report makes a similar recommendation for the entire industrial base: "Congress should direct the U.S. government to develop and implement an industrial base strategy for information and communications technology to ensure trusted supply chains."[68]

The development of the *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* was motivated by the realization that, currently, there is no way to assess the potential impact of a cyber supply chain event.[69] This lack of ability to assess, rank, or quantify supply chain risk is especially troubling considering that supply changes for electronic components are interconnected, as shown in Figures 3 and 4 and other knowledge graphs available on the web. The purpose of the impact analysis tool is to provide a way to rate these risks.

In the tool's methodology, each node in the company's supply chain has three scores: impact, interdependence, and assurance. These scores are derived from the user's answers to a questionnaire. (See Appendix B for the list of questions.) Some of the questions are about the supplier's access: For example, does the supplier have access to the information technology network, physical facility, or sensitive data? Other questions are about the supplier's assurance: How long has the supplier been in business? Does the supplier follow appropriate industry standards? Is the supplier owned by a foreign country or competitor?

Another part of the questionnaire relates to the product. These questions are about access, criticality, and dependence. For example, is the product critical to the project, and is the product used in more than one project? How much of the product comes from each supplier, and how much of the supplier's sales come from this product? Would switching to another supplier increase cost? What is the degree of confidence the product can be obtained if there is a supply chain disruption?

A node's impact score has a value between 0 and 100, with 0 indicating no impact and 100 indicating ruin. It is the sum of the maximum dependency score and the maximum access scores for each supply line to that node. A node's interdependence score is the sum of the dependency and access scores for each supply line to that node. This score is unbounded. The assurance score is a percentage indicating the number of SCRM actions the supplier has implemented out of all possible actions. Lower scores indicated fewer mitigations.

To display these scores, the tool has both a box-and-whisker graph (Figure 5) and a scatter plot (Figure 7) that help the user quantify and rank the risks in their supply chain. These two graphs are generic versions of Figures 18 and 19 in the draft impact analysis tool (NIST IR 8272).[70] Here, we

FIGURE 5

Box and Whisker Graph of Five Suppliers' Product Impact Scores

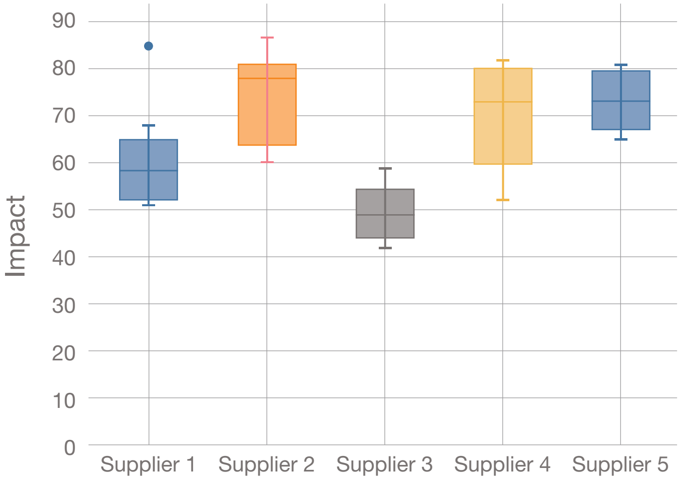
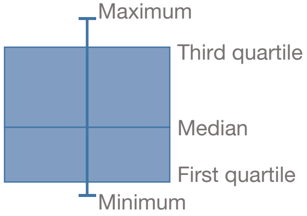


FIGURE 6

Parts of a Box and Whisker Plot



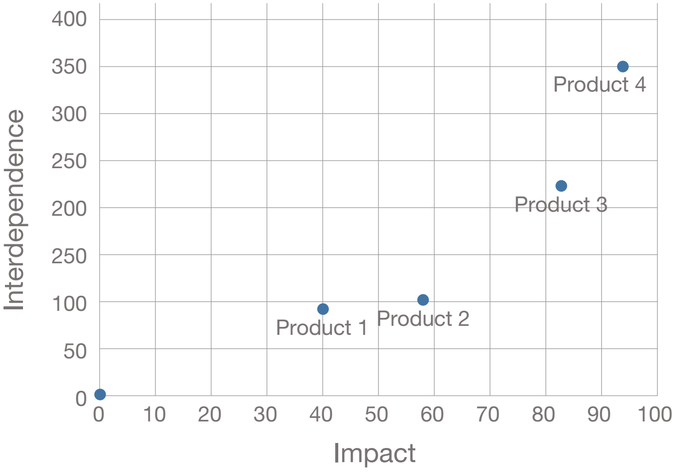
provide notional examples, along with a diagram (Figure 6) of how to read a box-and-whisker graph.

For each supplier, Figure 5 displays the impact that the supplier's parts have on the product. The NIST IR states that "the impact Score represents the highest potential negative impact a node can have on the organization if it fails."[71] The scores can therefore provide a view into which suppliers are most critical to a manufacturer. The five summary markers indicating a score on the *y* axis presented on each box and whisker set are the minimum, first quartile, median, third quartile, and maximum (see Figure 6). The first supplier's minimum and first quartile scores are almost identical at 51; the median is at 58 and the fourth quartile at 65 with a maximum impact score of 85. Supplier 2 has the highest maximum impact score of 87. Supplier 3 has the lowest overall impact based on these scores. The tool's impact scores range between 0 and 100; a higher score indicates a more negative potential impact on the organization should the supplier be compromised. To mitigate a high impact score, the organization can reduce dependence on that supplier, work with the supplier to reduce the risk their product poses and limit the supplier's access to data and networks.

Figure 7 displays a scatter plot of the impact score (horizontal axis) versus the interdependence score (vertical axis) for each product. The interdependence score indicates the node's influence in the organization's supply chain. A supplier that provides many products to an organization has a higher interdependence score than a supplier of one or two products has. For each product that has one supplier and one project, the impact score equals the interdependence score. Products in the upper right of the

FIGURE 7

Scatter Plot of Four Products' Interdependency Scores



plot (so here, product 4) are those of highest impact and interdependence. The tool's interdependence score is determined by the structure of organization's supply chain. The score indicates the degree to which the organization depends on current suppliers for the product. To decrease the interdependence score, the organization should expand the number of suppliers for that product.

Faced with complex and interdependent election infrastructure, election officials may not know where to concentrate efforts to reduce risk of cyber attacks. These visualizations help identify where to focus risk mitigation strategies by showing the interconnections between nodes, as well as the most-significant nodes in the supply chain.[72]

Conclusion

Cyber SCRM is a daunting prospect regardless of sector: in the commercial world, across the federal government, in the defense sector, or for elections. This developing field has seen many recent innovative approaches to improving the cybersecurity for supply chains in general and the U.S. election supply chain specifically. The application of these new approaches occurs at all levels of the election supply chain across the vendor community, as well as in federal, state, and local organizations, and requires collaboration across these levels. The following actions should be taken to continue the improvement of cyber SCRM for election infrastructure.

- Election officials, in partnership with the federal government and vendors, should apply the six essential steps in the CISA *SCRM Essentials* as shown in Appendix A. For those unaccustomed to thinking about supply chain management, the CISA guide is a useful first step. This will require ensuring that trained and empowered personnel at the federal, state, and local levels have the resources and access to information to implement this approach.
- State and local election officials should continue to take advantage of CISA services for protecting election infrastructure, sharing intelligence, and identifying threats.
- Although the NIST impact analysis tool is still under development, both EAC and DHS should begin using this tool to support piloting and refining the tool with selected state and local election officials as they seek to understand and manage risk in their supply chains. This might require additional funding for continued application. Once the tool has been applied to a particular supply chain, it will be possible to rank the supplier's risk. Users will need to use this new tool before they can be confident in the results. This is a beginning for SCRM risk management.
- EAS and DHS should work to develop supply chain visualizations using data from the NIST

tool and from the knowledge graph (BOKN) database. Making use of such visualizations will improve cyber incident reporting by tracing the links in overlapping supply chains.

- EAC should certify suppliers like it certifies labs that test voting equipment. Such certification would help establish bidirectional sharing of information.
- Election equipment purchasers across the states should band together or work through EAC to accredit those suppliers or switch to ones that are accredited.
- States should be made aware of compliance.
- EAC voting system guidelines should be updated to incorporate both supplier certification and SCRM.

These are a few practical steps that the federal government, state and local governments, and the vendor community can use with existing approaches and tools to collectively advance cyber SCRM for election systems.

Appendix A. Implementing Cybersecurity and Infrastructure Security Agency Supply Chain Risk Management Essentials

The tables in this appendix outline the process needed to implement the six essential steps in CISA's *SCRM Essentials*. Tables A.1, A.2, and A.3 address the federal, state, and local levels, respectively. Each of the six steps corresponds to one row in each table. The actions required to help mitigate risk are listed in the second column. The remaining columns, which the user fills in for each system component while completing the steps the process, are the elements of the election system.

TABLE A.1

Federal Level

		Registration		Election Machines		
Step	Action	Voter Registration	Pollbooks	Voting Machines	High-Speed Scanners	Tabulation
Identify: Determine who from the organization needs to be involved.	For each state, maintain a list of responsible people.					
Manage: Develop supply chain security policies and procedures.	Set security standards based on those used in DoD and government.					
Assess: Understand the hardware, software, and services being procured.	Maintain data on all companies supplying election hardware, software, and services. Publish all software updates.					
Know: Map the supply chain to better understand what components are being procured.	Maintain a list of tier 1 suppliers for all election and software equipment.					
Verify: Determine how the organization will assess a supplier's security culture.	Expand the EAC certification program to include vendors supplying parts and software for election machines.					
Evaluate: Establish systems for checking supply chain practices against guidelines.	Establish a schedule for compliance verification. Maintain a database of compliance actions and breaches.					

TABLE A.2

State Level

		Registration		Election Machines		
Step	Action	Voter Registration	Pollbooks	Voting Machines	High-Speed Scanners	Tabulation
Identify: Determine who from the organization needs to be involved.	For each county, identify responsible people across organizations.					
Manage: Develop supply chain security policies and procedures.	Know security standards set at the federal level. Train all personnel in security measures.					
Assess: Understand the hardware, software, and services being procured.	Provide EAC with data on all companies supplying election hardware, software, and services in the state.					
Know: Map the supply chain to better understand what components are being procured.	Maintain a list of tier 1 suppliers for unique election and software equipment in the state, and coordinate with the federal tier 1 list.					
Verify: Determine how the organization will assess a supplier's security culture.	Authenticate and update the currency of EAC certification of all election equipment.					
Evaluate: Establish systems for checking supply chain practices against guidelines.	Establish a schedule for compliance verification. Maintain a database of compliance actions and breaches.					

TABLE A.3

Local Level

		Registration		Election Machines		
Step	**Action**	**Voter Registration**	**Pollbooks**	**Voting Machines**	**High-Speed Scanners**	**Tabulation**
Identify: Determine who from the organization needs to be involved.	For each system, identify responsible people and positions across the organization.					
Manage: Develop supply chain security policies and procedures.	Know security standards set at the federal and state levels. Train all personnel in security measures.					
Assess: Understand the hardware, software, and services being procured.	Provide state election managers with data on all companies supplying election hardware, software, and services in that location.					
Know: Map the supply chain to better understand what components are being procured.	Maintain a list of tier 1 suppliers for unique election and software equipment in that location and coordinate with the state tier 1 list					
Verify: Determine how the organization will assess a supplier's security culture.	Authenticate and update the currency of EAC certification of all election equipment.					
Evaluate: Establish systems for checking supply chain practices against guidelines.	Establish a schedule for compliance verification. Maintain a database of compliance actions and breaches.					

Appendix B. Impact Analysis Tool Questions

The details of how the answers to these questions are used to calculate scores are described in the appendixes to NIST IR 8272.[73] The installer package, sample data sets, and source code for the tool are available on the NIST website.[74]

Product Questions

Criticality

1. What is the criticality of this {product/service} to the {project} [Project ID]?

Access

1. Is this {product/service} connected to or a part of your company's systems/networks?
2. Is this {product/service} connected to or a part of a product or service that your company provides to customers?
3. Does this {product/service} process or store regulated data (e.g., PII, PHI [protected health information, PCI [payment card industry], etc.) or your company's sensitive information (e.g., intellectual property, financial data, internal processes, etc.)?

Dependency

1. What is the {supplier}'s ([Supplier ID]) market share for this particular {product/service}?
2. What percent of the {supplier}'s ([Supplier ID]) sales of this {product/service} does your company consume?
3. Would switching to an alternative {supplier} constitute significant cost or effort for your company?
4. Does your company have an existing relationship with another {supplier} for this {product/service}?
5. How confident is your company that [it] will be able to obtain quality {products/services} regardless of major supply chain disruptions, both manmade and natural?
6. Does your company maintain a reserve of this {product/service}?

Project Question

Criticality

1. How critical is this {project} to your company's mission/business?

Supplier Questions

Access

1. Does {supplier} have access to your company's IT [information technology] networks, OT [operational technology] systems, or sensitive platforms (e.g., payment portals)?
2. Does {supplier} have access to . . . your company's physical facilities?

3. Does {supplier} have access to your company's sensitive information (e.g., intellectual property, financial data, internal processes, etc.) or regulated data (e.g., PII, PHI, PCI, etc.) for which your company is responsible?

Assurance

1. Does the {supplier} have fewer than 10 employees?
2. How long has this {supplier} been in business?
3. How much of the {supplier}'s total business is provided by your company?
4. Does this {supplier} follow relevant industry standards?
5. Does this {supplier} operate in highly regulated industries or provides products/services to highly regulated industries (e.g., Financial services, Energy)?
6. Is the {supplier} owned, controlled, or influenced in full or in part by an entity of concern (e.g. foreign nation state, competitors)?
7. How sensitive is the {supplier}'s ability to provide quality products/services to supply chain disruptions, both manmade and natural?
8. Has this {supplier} filled out a questionnaire to qualify for providing products or services to your company?
9. Has your company verified the information provided by the {supplier} on their supplier questionnaire?
10. Is your company able to influence this {supplier}'s security practices through supplier agreements?
11. Does your company know this {supplier}'s sub-suppliers?
12. Has the {supplier} provided your company with mitigation assurances (e.g. insurance, fallback partnerships with other vendors, etc)?

Notes

[1] Committee on House Administration, 2020.

[2] Interos, 2019. See also Allgeier, 2019.

[3] CQ Congressional Transcripts, 2020.

[4] U.S. Department of Homeland Security (DHS), 2017.

[5] U.S. Department of Homeland Security, 2018, p. 11.

[6] McNamara, 2019. Prior work is in Hodgson, Chan, et al., forthcoming.

[7] The considerations for the safe conduct of elections in pandemic conditions are addressed in Hodgson, Kavanagh, et al., 2020.

[8] For concision, we use the term *state and local* to also encompass territorial and tribal officials.

[9] U.S. Constitution, Art. I, § 4.

[10] U.S. Constitution, Art. II, § 1.

[11] This is not intended to imply that the state has no role to play—only that California is less centralized than other states. For example, when Los Angeles County decided to develop and deploy an entirely new election system, the state provided conditional certification of that system that laid out a series of steps the county had to take. See Padilla, 2020.

[12] CISA, undated.

[13] Center for Internet Security, undated.

[14] Pub. L. 107-252.

[15] EAC, undated a.

[16] Software Quality Group, 2019.

[17] Information Technology Laboratory, undated.

[18] CISA, 2019.

[19] Blaze et al., 2019, p. 3.

[20] National Association of Secretaries of State, 2018.

[21] CISA, 2020c.

[22] Exposing the contents of an individual ballot could be a concern, although, absent the ability to tie the ballot to an individual, the impact of such exposure would be limited. Aside from ballots, some data held in election systems (e.g., personally identifiable information, or PII, in voter registration records; sensitive information that some states protect, such as home addresses for judges and law enforcement officers) are not intended for public release, but this is a lesser attack concern for the most part.

[23] For recent RAND work on the topic, see Hodgson, Chan, et al., forthcoming.

[24] See ERIC, undated.

[25] For examples of how this affects the voting machine technology, see Verified Voting, undated.

[26] Verified Voting, undated.

[27] Verified Voting, undated.

[28] Verified Voting, undated.

[29] Rexaline, 2019.

[30] On the difficulty in detecting hardware manipulation, see Crouch, Hunter, and Levin, 2018.

[31] Robertson and Riley, 2018.

[32] Wemple, 2018.

[33] Elkins, 2018.

[34] Interos, 2018, p. 6. The supply chain tiers are parts (tier 1), components (tier 2), and modules or systems (tier 3).

[35] As evidenced by, for example, the Help America Vote Act of 2002 (Pub. L. 107-252) and the designation of elections as critical infrastructure.

[36] This concern has been highlighted recently with police body cameras that still had recordings on them when found for sale online (Rose, 2020).

[37] "According to one estimate, in 1946 only 20% of a typical American manufacturing company's value-added in production and operations came from outside sources; 50 years later the proportion had tripled to 60%" ("Outsourcing," 2008).

[38] NIST, undated a.

[39] Published in April 2015, SP 800-161 (Boyens, Paulsen, Moorthy et al., 2015), "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," was undergoing revision as of February 2020. See Boyens, Paulsen, Moorthy et al., 2015, for news and updates.

[40] CISA, 2018b; CISA, 2018c.

[41] Paulsen et al., 2020.

[42] CISA, 2020a.

[43] Boyens, Paulsen, Bartol, et al., 2020a.

[44] Pub. L. 107-252, 2002, § 231(a)(1).

[45] EAC, 2015, p. i.

[46] Hart InterCivic, undated.

[47] Zetter, 2019.

[48] Geller, 2020.

[49] Howard, 2020.

[50] Under Secretary of Defense for Acquisition and Sustainment, 2019.

[51] Norden, Deluzio, and Ramachandran, 2019.

[52] Dun and Bradstreet, undated.

[53] Boeing Corporation, 2020; Lockheed Martin Corporation, 2020.

[54] CISA, 2020b.

[55] DHS, 2017.

[56] Defense Microelectronics Activity, 2020.

[57] Machines are built over time, and suppliers change. So a machine might have been certified in 2016, but new machines of the same model built in 2018 might fail certification. With this accreditation process in place, a state does not need to verify individual machines itself.

[58] EAC, undated b.

[59] Boyens, Paulsen, Moorthy, et al., 2015.

[60] Boyens, Paulsen, Moorthy, et al., 2015, p. 2.

[61] Toth, 2017.

[62] Boyens, Paulsen, Bartol, et al., 2020a.

[63] Paulsen et al., 2020.

[64] U.S. Government Accountability Office, 2020.

[65] Center on Knowledge Graphs, undated.

[66] Knowledge graphs are a product of The Business Open Knowledge Network (BOKN) funded by the National Science Foundation to promote multidisciplinary collaboration and real-world impact.

[67] Van der Staak and Wolf, 2019.

[68] U.S. Cyberspace Solarium Commission, 2020, p. 12.

[69] Paulsen et al., 2020.

[70] Paulsen et al., 2020.

[71] Paulsen et al., 2020, p. 29.

[72] The data underlying the visualizations come from detailed user-completed questionnaires; Excel files containing details about suppliers, products, and projects; and basic information about the structure of the organization's supply chain. Each node is given a user-assessed score of impact, interde-

pendence, and assurance. These scores are derived from the information in the questionnaire.

[73] Paulsen et al., 2020.

[74] Information Technology Laboratory, 2020.

Bibliography

Allgeier, Harris, "Interos Study of Widely-Used Voting Machine Finds 1 in 5 Components from China-Based Companies," Interos, December 16, 2019. As of February 26, 2020:
https://www.interos.ai/voting-study/

Blaze, Matt, Harri Hursti, Margaret MacAlpine, Mary Hanley, Jeff Moss, Rachel Wehr, Kendall Spencer, and Christopher Ferris, *DEF CON 27 Voting Machine Hacking Village*, DEF CON, August 2019.

Boeing Corporation, "Boeing Reports Fourth-Quarter Results," press release, January 29, 2020. As of July 15, 2020:
https://investors.boeing.com/investors/investor-news/press-release-details/2020/Boeing-Reports-Fourth-Quarter-Results/default.aspx

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, National Institute of Standards and Technology, U.S. Department of Commerce, draft Interagency or Internal Report 8276, February 2020a. As of August 20, 2020:
https://csrc.nist.gov/publications/detail/nistir/8276/draft

———, *Case Studies in Cyber Supply Chain Risk Management: Observations from Industry—Summary of Findings and Recommendations*, Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, February 4, 2020b. As of August 19, 2020:
https://csrc.nist.gov/publications/detail/white-paper/2020/02/04/case-studies-in-c-scrm-summary-of-findings-and-recommendations/final

Boyens, Jon, Celia Paulsen, Rama Moorthy, and Nadya Bartol, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," Computer Security Resource Center, Information Technology Laboratory, National Institute of Standards and Technology, Special Publication 800-161, April 2015. As of August 21, 2020:
https://csrc.nist.gov/publications/detail/sp/800-161/final

Center for Internet Security, "Elections Infrastructure ISAC," webpage, undated. As of July 13, 2020:
https://www.cisecurity.org/ei-isac/

Center on Knowledge Graphs, Information Sciences Institute, University of Southern California, "Knowledge Graphs for Business," website, undated. As of August 1, 2020:
https://usc-isi-i2.github.io/bokn/

CISA—*See* Cybersecurity and Infrastructure Security Agency.

Committee on House Administration, U.S. House of Representatives, "2020 Election Security: Perspectives from Voting System Vendors and Experts," hearing announcement, January 9, 2020. As of February 26, 2020:
https://cha.house.gov/committee-activity/hearings/2020-election-security-perspectives-voting-system-vendors-and-experts

CQ Congressional Transcripts, "House Administration Committee Holds Hearing on Election Security," January 9, 2020.

Crouch, Alfred, Eve Hunter, and Peter L. Levin, "Enabling Hardware Trojan Detection and Prevention Through Emulation," *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, Woburn, Mass., 2018, pp. 1–5.

Cybersecurity and Infrastructure Security Agency, "About CISA," webpage, undated. As of June 30, 2020:
https://www.cisa.gov/about-cisa

———, *Elections Infrastructure Subsector–Specific Plan: An Annex to the NIPP 2013*, 2018a. As of August 28, 2020:
https://www.cisa.gov/sites/default/files/publications/election_infrastructure_subsector_specific_plan.pdf

———, "DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force," press release, October 30, 2018b. As of February 26, 2020:
https://www.cisa.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology

———, "DHS Announces ICT Supply Chain Risk Management Task Force Members," press release, November 15, 2018, last revised November 19, 2018c. As of February 26, 2020:
https://www.cisa.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members

———, "Government Facilities Sector—Election Infrastructure Subsector: Charters and Membership," webpage, last revised May 8, 2019. As of July 7, 2020:
https://www.cisa.gov/government-facilities-election-infrastructure-charters-and-membership

———, *SCRM Essentials: Information and Communications Technology Supply Chain Risk Management (SCRM) in a Connected World*, May 2020a. As of July 8, 2020:
https://www.cisa.gov/sites/default/files/publications/ict_scrm_essentials_508.pdf

———, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force," webpage, last revised June 15, 2020b. As of July 15, 2020:
https://www.cisa.gov/ict-scrm-task-force

———, *Guide to Vulnerability Reporting for America's Election Administrators*, last revised July 31, 2020c. As of August 1, 2020:
https://www.cisa.gov/publication/election-vulnerability-reporting-guide

Defense Federal Acquisition Regulation Supplement, Part 252, Clauses; Subpart 252.2, Text of Provisions and Clauses; Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. As of August 21, 2020:
https://www.acquisition.gov/dfars/part-252-clauses#DFARS-252.204-7012

Defense Microelectronics Activity, Office of the Secretary of Defense, Trusted Foundry Program, "Accredited Suppliers," as of July 2, 2020. As of August 19, 2020:
https://www.dmea.osd.mil/otherdocs/accreditedsuppliers.pdf

DFARS—*See* Defense Federal Acquisition Regulation Supplement.

DHS—*See* U.S. Department of Homeland Security.

Dun and Bradstreet, "Business Directory," webpage, undated. As of May 18, 2020:
https://www.dnb.com/business-directory.html

EAC—*See* U.S. Election Assistance Commission.

Electronic Registration Information Center, homepage, undated. As of August 19, 2020:
https://ericstates.org

Elkins, Monta, hacker-in-chief, FoxGuard Solutions, "Jumping Air Gaps," talk delivered at SANS Europe Institute Industrial Control System Cyber Security Summit, June 14, 2018. As of July 9, 2020:
https://www.youtube.com/watch?v=XHJI0J2CMs4

ERIC—*See* Electronic Registration Information Center.

Geller, Eric, "Doublecheck That Ballot: Controversial Voting Machines Make Their Primary Debut in South Carolina," *Politico*, February 28, 2020. As of August 21, 2020:
https://www.politico.com/news/2020/02/28/south-carolina-voting-machines-118046

Hart InterCivic, "At Hart, Election Security Is in Our DNA," webpage, undated. As of July 8, 2020:
https://www.hartintercivic.com/electionsecurity/

Hicks, Thomas, "Defending and Recovering American Election Systems," *Brown Journal of World Affairs*, Vol. 24, No. 2, Spring–Summer 2018, pp. 97–108. As of August 19, 2020:
http://bjwa.brown.edu/24-2/defending-and-recovering-american-election-systems/

Hodgson, Quentin E., Edward W. Chan, Elizabeth Bodine-Baron, Bryan Boling, Benjamin Boudreaux, Bilyana Lilly, and Andrew J. Lohn, *Securing U.S. Elections: A Method for Prioritizing Cybersecurity Risk in Election Infrastructure*, Homeland Security Operational Analysis Center operated by the RAND Corporation, forthcoming.

Hodgson, Quentin E., Jennifer Kavanagh, Anusree Garg, Edward W. Chan, and Christine Sovak, *Options for Ensuring Safe Elections: Preparing for Elections During a Pandemic*, Santa Monica, Calif.: RAND Corporation, RR-A112-10, 2020. As of August 20, 2020:
https://www.rand.org/pubs/research_reports/RRA112-10

Howard, Elizabeth L., counsel, Democracy Program, Brennan Center for Justice, New York University School of Law, *2020 Election Security: Perspectives from Voting System Vendors and Experts*, statement for the U.S. House of Representatives Committee on Administration, January 9, 2020. As of August 19, 2020:
https://www.brennancenter.org/our-work/research-reports/congressional-testimony-2020-election-security-and-election-vendors

Information Sciences Institute, Viterbi School of Engineering, University of Southern California, *Delivering the Future: 2019 Annual Report*, c. 2020.

Information Technology Laboratory, Computer Security Resource Center, National Institute of Standards and Technology, "Voting," website, undated. As of June 30, 2020:
https://www.nist.gov/itl/voting

———, "Cyber Supply Chain Risk Management C-SCRM," created May 24, 2016; updated June 22, 2020. As of August 21, 2020:
https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/interdependency_tool

Interos, "Election Technology and the Global Supply Chain," December 2019. As of February 26, 2020:
https://cdn2.hubspot.net/hubfs/5812029/Interos%20-%20Election%20Security%20Paper.pdf

Lockheed Martin Corporation, "Lockheed Martin Reports Fourth Quarter and Full Year 2019 Results," press release, January 28, 2020. As of July 15, 2020:
https://news.lockheedmartin.com/2020-01-28-Lockheed-Martin-Reports-Fourth-Quarter-and-Full-Year-2019-Results

McNamara, Luke, "Framing the Problem: Cyber Threats and Elections," *Fireeye*, May 30, 2019. As of August 19, 2020:
https://www.fireeye.com/blog/threat-research/2019/05/framing-the-problem-cyber-threats-and-elections.html

National Association of Secretaries of State, "NASS Statement on DEFCON Voting Machine Hacking Events," press release, Washington, D.C., August 9, 2018. As of August 19, 2020:
https://www.nass.org/node/1511

National Institute of Standards and Technology, "Information and Communications Technology Supply Chain Risk Management (ICT SCRM)," fact sheet, undated a. As of February 26, 2020:
https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf

———, *Best Practices in Cyber Supply Chain Risk Management: Boeing and Exostar, Cyber Security Supply Chain Risk Management*, undated b. As of August 19, 2020:
https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf

NIST—*See* National Institute of Standards and Technology.

Norden, Lawrence, Christopher R. Deluzio, and Gowri Ramachandran, *A Framework for Election Vendor Oversight: Safeguarding America's Election Systems*, New York: Brennan Center for Justice at New York University, November 12, 2019. As of August 19, 2020:
https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight

"Outsourcing," *The Economist*, September 29, 2008. As of August 21, 2020:
https://www.economist.com/news/2008/09/29/outsourcing

Padilla, Alex, California Secretary of State, letter to Dean Logan, Registrar-Recorder/County Clerk, Los Angeles County, transmitting conditional approval of the county's Voting Solutions for All People 2.0 voting system, January 24, 2020. As of August 19, 2020: https://votingsystems.cdn.sos.ca.gov/vendors/LAC/vsap20-cert.pdf

Paulsen, Celia, Jon Boyens, Jeffrey Ng, Kris Winkler, and James Gimbi, *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks*, Gaithersburg, Md.: National Institute of Standards and Technology, draft Interagency or Internal Report 8272, March 2020. As of March 19, 2020: https://csrc.nist.gov/publications/detail/nistir/8272/draft

Public Law 107-252, Help America Vote Act of 2002, October 29, 2002. As of August 19, 2020: https://www.govinfo.gov/app/details/PLAW-107publ252

Rexaline, Shanthi, "Intel Vs. AMD: Reviewing the Rivalry as CPU Market Shares Shift," *Yahoo! Finance*, December 31, 2019. As of August 19, 2020: https://finance.yahoo.com/news/intel-vs-amd-reviewing-rivalry-160718187.html

Robertson, Jordan, and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg Businessweek*, October 4, 2018. As of June 30, 2020: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Rose, Janus, "Hackers Are Finding Footage on Police Body Cams They Bought on eBay," *Motherboard: Tech by Vice*, July 8, 2020. As of August 21, 2020: https://www.vice.com/en_us/article/8895ek/hackers-are-finding-footage-on-police-body-cams-they-bought-on-ebay

Software Quality Group, Software and Systems Division, Information Technology Laboratory, National Institute of Standards and Technology, "National Software Reference Library (NSRL)," updated November 18, 2019. As of August 19, 2020: https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl

Toth, Patricia R., *NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, U.S. Department of Commerce, National Institute of Standards and Technology, Handbook 162, November 20, 2017. As of August 19, 2020: https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security

Under Secretary of Defense for Acquisition and Sustainment, U.S. Department of Defense, "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review," memorandum for commander, U.S. Cyber Command; commander, U.S. Special Operations Command; commander, U.S. Transportation Command; Assistant Secretary of the Army for Acquisition, Logistics, and Technology; Assistant Secretary of the Navy for Research, Development, and Acquisition; Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics; directors of the defense agencies; and directors of the U.S. Department of Defense field activities, January 21, 2019. As of August 19, 2020: https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf

U.S. Code, Title 10, Armed Forces; Subtitle A, General Military Law; Part IV, Service, Supply, and Procurement; Chapter 148, National Defense Technology and Industrial Base, Defense Reinvestment, and Defense Conversion; Subchapter V, Miscellaneous Technology Base Policies and Programs; Section 2533a, Requirement to Buy Certain Articles from American Sources; Exceptions. As of August 19, 2020:
https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section2533a&num=0&edition=prelim

U.S. Cyberspace Solarium Commission, official final report, March 2020. As of August 19, 2020:
https://www.solarium.gov

U.S. Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," press release, January 6, 2017. As of July 10, 2020:
https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

———, "Removal of Kaspersky-Branded Products," Binding Operational Directive 17-01, September 13, 2017. As of August 19, 2020:
https://cyber.dhs.gov/bod/17-01/

U.S. Election Assistance Commission, "About the U.S. EAC," website, undated a. As of June 30, 2020:
https://www.eac.gov/about-the-useac

———, "Voting Equipment: Voluntary Voting System Guidelines," website, undated b. As of July 15, 2020:
https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

———, *Testing and Certification Program Manual*, version 2.0, Office of Management and Budget Control 3265-0019, effective May 31, 2015. As of August 19, 2020:
https://www.eac.gov/sites/default/files/eac_assets/1/6/Cert_Manual_7_8_15_FINAL.pdf

U.S. Government Accountability Office, *Election Security: DHS Plans Are Urgently Needed to Address Identified Challenges Before the 2020 Elections*, Washington, D.C., GAO-20-267, February 6, 2020. As of August 19, 2020:
https://www.gao.gov/products/GAO-20-267

Van der Staak, Sam, and Peter Wolf, *Cyber Security in Elections: Models of Interagency Collaboration*, Stockholm: International Institute for Democracy and Electoral Assistance, July 19, 2019. As of August 19, 2020:
https://www.idea.int/publications/catalogue/cybersecurity-in-elections

Verified Voting, "The Verifier: Polling Place Equipment—November 2020," webpage, undated. As of July 8, 2020:
https://www.verifiedvoting.org/verifier/

Wemple, Erik, "Bloomberg Is Still Reporting on Challenged Story Regarding China Hardware Hack," *Washington Post*, opinion, November 27, 2018.

Zetter, Kim, "Experts: Elections Commission Downplaying Unseen Risks to 2020 Vote," *Politico*, March 15, 2019. As of August 19, 2020:
https://www.politico.com/story/2019/03/15/election-machine-security-2020-cybersecurity-1222803

About This Perspective

The cybersecurity of election systems has long been a central focus of election officials and the federal government, starting with the passage of the Help America Vote Act in 2002 (Pub. L. 107-252) and more recently in 2017 with the designation of elections as a critical infrastructure subsector. Federal partners in the Cybersecurity and Infrastructure Security Agency, the U.S. Election Assistance Commission, and the National Institute of Standards and Technology are supporting the election community, including election officials and vendors, to improve cybersecurity. More recently, this focus has expanded to concerns about the supply chain of components that are integral to election system equipment. This concern for the cybersecurity of supply chains is found throughout industry as organizations strive to protect their equipment and customers from cyber threats. In this Perspective, RAND Corporation researchers lay out the considerations for securing election system supply chains against cyber threats and how the federal government can partner with state and local officials and the vendor community to understand where risk lies in the supply chain. The Perspective discusses how existing tools and approaches can be adapted and used to facilitate cyber supply chain risk management. It should be of interest to federal, state, and local election officials who will manage their relationships with the manufacturers of election equipment; to manufacturers that will, in turn, manage their relationships with their suppliers; and to those developing tools for mapping supply chains and assessing supply chain risk.

This research was conducted within the Strategy, Policy, and Operations Program of the RAND Homeland Security Research Division (HSRD). HSRD conducts research and analysis for the U.S. homeland security enterprise and serves as the platform by which RAND communicates relevant research from across its units with the broader homeland security enterprise.

For more information on the RAND Strategy, Policy, and Operations Program, see www.rand.org/hsrd.html or contact the program director (contact information is provided on the webpage).

About the Authors

Quentin E. Hodgson is a senior international and defense researcher at the RAND Corporation focusing on cybersecurity, cyber operations, critical infrastructure protection, risk management, and command and control. He holds an M.A. in international relations and an M.Sc. in national resource management and was a Fulbright scholar.

Marygail K. Brauner is a senior operations researcher at RAND. Her current research helps inform the rebuilding of Puerto Rico using evidence-based analysis, and past research has focused on military force planning and logistics. Brauner has a Ph.D. in engineering and operations research.

Edward W. Chan is a senior operations researcher at RAND. Chan's research has focused on the intersection of logistics problems with homeland security, public health, and emergency preparedness problems. Chan earned his Ph.D. in operations research.

For more information on this publication, visit www.rand.org/t/PEA512-1.

RAND CORPORATION

www.rand.org