SECURING THE GRID
FROM SUPPLY-CHAIN BASED ATTACKS

Paul N. Stockton (pstockton@sonecon.com)[1]

September 2, 2020

I. EXECUTIVE SUMMARY

The bulk power system (BPS) faces increasingly severe threats from China, Russia, and other potential adversaries. Executive Order (EO) 13920, *Securing the United States Bulk-Power System* focuses on a threat of special significance for US security: the corruption of supply chains for BPS equipment, and the danger that adversaries will use compromised equipment to cut off the flow of power to Defense installations and other critical facilities.[2] Countering this threat will require an innovative, comprehensive strategy to implement the EO.

The best way to achieve the EO's goals is to leverage the comparative advantages of DOE and its industry partners, and capitalize on their different but complementary responsibilities. BPS entities have detailed knowledge of their own systems, including Defense Critical Electric Infrastructure (DCEI), and have primary responsibility for the safe and reliable operation of them.[3] However, these entities should not have primary responsibility to determine which products on the market pose the greatest risk. Vendors have far better knowledge of the subcontractors who contribute to their products and their compliance with supply chain risk management (SCRM) standards. DOE and its intelligence community (IC) partners can and should routinely provide additional data on equipment and adversary efforts to penetrate supply chains and clarify how adversaries are likely to conduct supply chain-based attacks in the future. However, new approaches will be necessary to address the information sharing and liability challenges that EO implementation will entail.

Federal and state regulators can make vital contributions to implementation as well. In particular, regulators need data and analytic support to help them assess proposed utility purchases of more secure equipment, even if that equipment is more costly than alternatives intentionally underpriced by China and the other "foreign adversaries" specified in the DOE's Request for Information (RFI) on *Securing the United States Bulk-Power System*.[4] Doing so in ways that account for equity issues involved in ratepayer funding of national security-focused initiatives will also require input from regulators.

---

[1] Paul Stockton is Managing Director of Sonecon, LLC, and is a member of the Department of Energy's Electricity Advisory Council. He is a member of the Idaho National Laboratory's Strategic Advisory Committee and the Laboratory's Science and Technology Committee. He served as Assistant Secretary of Defense for Homeland Defense from 2009-2013. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

[2] White House, *Executive Order on Securing the United States Bulk-Power System*, May 1, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

[3] The *Federal Power Act* (FPA) defines DCEI as any infrastructure that serves facilities that are "critical to the defense of the United States" and are vulnerable to the disruption of grid-provided power, but are not owned by the owner or operator of that facility. See: 16 U.S.C. § 824o–1, Section (a)(4), https://www.law.cornell.edu/uscode/text/16/824o-1. Pursuant to the FPA, DOE is informing utilities of the DCEI within their systems.

[4] Department of Energy (DOE), *Securing the United States Bulk-Power System*, Federal Register Vol. 85, No. 131 (July 8, 2020): 41,024, https://www.govinfo.gov/content/pkg/FR-2020-07-08/pdf/2020-14668.pdf.

No organizational framework exists to coordinate DOE's implementation efforts with these diverse stakeholders and help them achieve unity of effort. The Order establishes a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security. While that Task Force enables consultations with industry councils, its responsibilities are far too narrow to achieve the Order's national security objectives.[5] Instead, building on collaborative arrangements already established by the Electricity Subsector Coordinating Council (ESCC), the North American Transmission Forum (NATF), and other organizations noted in this report, DOE and its partners should create an organizational framework to lead and coordinate EO implementation activities for many years to come.

These partners and many individual BPS entities and vendors already have strong SCRM initiatives underway, including mandatory standards, voluntary risk management frameworks, and mechanisms for information sharing. Integrating their efforts to help guide and support EO implementation constitutes "low hanging fruit," especially in terms of leveraging their progress in reducing the risks that foreign adversaries will secretly acquire, penetrate, or otherwise compromise vendor subcontractors and manufacturing operations. The continued tightening of mandatory SCRM standards established by the North American Electric Reliability Corporation (NERC) and voluntary industry initiatives offer additional foundations for progress.[6]

Yet, given the intensifying threats to BPS equipment supply chains, DOE and its partners should also create additional layers of defense and develop innovative means to *disrupt* the use of BPS supply chains to prepare for and conduct attacks on the grid. The starting point to do so lies in: 1) analyzing the goals that such attacks will seek to achieve; 2) examining the implications for the design, insertion, and use of compromised BPS equipment; and 3) developing US countermeasures that exploit these adversary requirements and significantly increase the difficulty of attacking the grid. My report focuses on four such opportunities for progress:

- In coordination with industry, develop and share with industry a holistic, **operationally focused** assessment of the threat. The RFI cites the *National Counterintelligence Strategy of the United States of America* and other IC products in highlighting adversary efforts to corrupt critical supply chains.[7] These documents feature a finding of special significance for developing new approaches to BPS defense. The *Counterintelligence Strategy* emphasizes that adversary efforts to corrupt supply chains and related efforts to degrade critical systems "likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption."[8] Other government threat assessments warn that in a regional crisis, adversaries may also disrupt the US grid and

[5] White House, *Executive Order on Securing the United States Bulk-Power System*, Section 3. The EO specifies that the Task Force shall consult with the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council.

[6] For the NERC standard, see: North American Electric Reliability Corporation, *CIP-013-1 – Cyber Security – Supply Chain Risk Management*, July 2017, 3, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

[7] DOE, *Securing the United States Bulk-Power System*, 41,023.

[8] National Counterintelligence and Security Center (NCSC), *National Counterintelligence Strategy of the United States of America 2020-2022*, Washington, DC: Office of the Director of National Intelligence (ODNI), February 2020, 6, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

grid-dependent infrastructure to disrupt the deployment of forces to the crisis zone.[9] Threats to BPS supply chains and US initiatives to mitigate them under EO 13920 should be understood in this underlying, crisis-oriented context.

Most important: compromised BPS components are not "silver bullets" that will automatically achieve the effects that US opponents will seek in a crisis. If adversaries want to time and target grid disruptions to help them prevail in a confrontation with the US, they will face specialized requirements to prepare for and conduct supply-chain based attacks. Identifying these requirements will enable the US to develop innovative countermeasures. Doing so can also help industry and DOE better prioritize EO implementation measures, especially for protecting DCEI and preventing opponents from achieving their objectives in an attack.

- Develop a "kill chain" to further clarify supply chain attack requirements and identify specific defense opportunities. The US military creates kill chains to specify the steps necessary to target and attack an opponent to create the effects that the attacker seeks.[10] For cyberattacks, these sequential steps typically include intelligence gathering and planning, designing the cyberweapon, testing the weapon and/or modeling its effects, delivering and installing the weapon on the adversary's systems, and launching the attack.[11] Adversary efforts to leverage compromised BPS equipment during a crisis will entail specialized and demanding requirements for a number of these steps.

- For each of the steps in the compromised equipment (CE) kill chain, identify possible US countermeasures and pursue the options that provide the biggest "bang for the buck." The analysis that follows highlights one of many such options: exploiting adversary requirements to establish and maintain command and control (C2) over their malware or other compromises, which is a prerequisite for timing their attacks in future crises. Kill chains developed for cyber and industrial control system (ICS) attacks note that adversaries typically establish connectivity with corrupted devices to deliver commands or conduct other C2 activities.[12] If adversaries have similar requirements to prepare for and execute attacks that employ compromised BPS equipment, the ability to disrupt such C2 operations may create unique opportunities for grid defense. The use of a kill chain methodology will

[9] Department of Defense (DOD), *Mission Assurance Strategy*, Washington, DC: DOD, April 2012, http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.; Terrence O'Shaughnessy, Testimony Before the Senate Armed Services Committee, February 26, 2019, p. 2, https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-26-19.pdf; Bradley Peniston, "Work: 'The Age of Everything Is the Era of Grand Strategy,'" Defense One, November 2, 2015, http://www.defenseone.com/management/2015/11/work-age-everything-era-grand-strategy/123335/;

[10] This definition paraphrases the one provided in Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Bethesda, MD: Lockheed Martin, 2011, 4, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[11] Hutchins, Cloppert, and Amin, *Intelligence-Driven Computer Network Defense*, 5. Building on that cyber model, Assante and Lee developed a variant for ICS. Section 3 of this article proposes how their model can be further refined for application to supply chain threats.

[12] Hutchins, Cloppert, and Amin, *Intelligence-Driven Computer Network Defense*, 5; Michael Assante and Robert M. Lee, *The Industrial Control System Cyber Kill Chain*, Bethesda, MD: SANS Institute, 2015, 5, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

also facilitate broader risk assessment and mitigation efforts, including those necessary to counter adversary attempts to hide or minimize their C2 activities.

- Build a twofold strategy to block the insertion of compromised equipment. To provide industry with a list of prohibited equipment, the starting point should be to determine whether equipment or sub-components were produced by entities that entail foreign adversary "ownership, control, and influence."[13] In collaboration with vendors, BPS entities might also develop additional voluntary measures and best practices regarding the processes by which products are designed, developed, and produced, and help enable the Secretary to identify BPS equipment as "pre-qualified" for purchase.[14]

  Yet, adversaries are certain to pursue sophisticated means of evading these process-oriented safeguards. DOE and its partners should also ramp up testing and evaluation (T&E) programs for equipment which, if compromised, would inflict severe disruption on the grid. The CyTRICS program and other initiatives conducted by DOE National Laboratories provide a basis to build such a T&E system. But their testing throughput is tiny compared to the potential requirements for EO implementation. The analysis that follows recommends consequence-based methodologies to prioritize the testing of BPS equipment and propose options to build on current T&E programs to meet the BPS' long-term needs.

- Structure an organizational framework to help lead and coordinate EO implementation. Strengthening supply chain resilience will depend on contributions from vendors, their BPS customers, DOE, regulators, and a range of other partners. Attempting to establish centralized Federal control over all such participants would be a fool's errand. Instead, a voluntary organizational framework is necessary to help coordinate their efforts, build consensus to resolve implementation problems, and create unity of effort among them.

  Information sharing exemplifies the benefits of establishing such coordinating mechanisms. The EO will fail unless BPS entities and their partners get the data they need to contribute to the Order's implementation. However, data on supply chain threats is often highly classified and very few private sector personnel and state regulators have the clearances required to receive it. The sharing of equipment testing results and other sensitive information on BPS products could also create significant concerns for vendors, and – unless resolved – could limit vendors' willingness to provide their equipment for evaluation. Input from all of these stakeholders on their "need to know" sensitive data for EO implementation and their concerns and recommendations to protect that information will be essential for progress. Implementation partners can also help ensure that EO-related information complies with anti-trust laws and regulations and (for BPS entities) with CIP-011-2 – Information Protection.[15]

[13] DOE, Securing the United States Bulk-Power System, 41,024.

[14] White House, Executive Order on Securing the United States Bulk-Power System, Section 1(d). For an example of such voluntary SCRM frameworks for BPS entities to employ, see NCSC, Supply Chain Risk Management: A Framework for Assessing Risk, Washington, DC: ODNI, April 22, 2019, https://www.dni.gov/files/NCSC/documents/supplychain/20190422-SCRM-Framework-for-Assessing-Risk.pdf.

[15] North American Electric Reliability Corporation (NERC), CIP-011-2 – Cyber Security – Information Protection, effective July 1, 2016, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-011-2.pdf.

The ESCC, NATF, and other industry organizations already have established frameworks for collaboration. Building on these existing arrangements (rather than creating an organization from scratch) would be the least costly and most efficient way to facilitate industry coordination. But it will also be essential to ensure deep and sustained participation in such a coordinating body by DOE, the broader intelligence community, and other Federal departments and agencies. The EO's Task Force structure provides a starting point to organize for such collaboration over a far broader range of topics than those specified by the Order. The key is that the coordinating body would: 1) be dedicated to SCRM; 2) include the full range of partners necessary to help counter supply chain-based attacks, including vendors and the regulators who will play crucial roles in enabling cost recovery for more secure equipment; and 3) be structured and funded for the multi-year effort required to defeat supply chain threats.

II. DEVELOPING AND SHARING A HOLISTIC THREAT ASSESSMENT

Industry's most pressing need for intelligence support from DOE and its IC partners lies in identifying the high-risk equipment that companies will be barred from purchasing under the EO, Power companies are making procurement decisions now for transformers that are often purpose-built and may not be delivered and installed until years after they are ordered. Those extended timelines put companies at risk of buying products that may subsequently be prohibited.

BPS entities also need DOE, IC, and vendor expertise in determining whether they have at-risk equipment in their existing DCEI systems. The EO requires the Secretary of Energy to "develop recommendations on ways to identify, isolate, monitor, or replace such items as soon as practicable, taking into consideration overall risk to the bulk-power system."[16] Input from the electric industry will be essential for developing such recommendations, including mechanisms for cost recovery if at-risk equipment must be replaced. Nevertheless, DOE and its Federal partners must help BPS entities target and prioritize their searches for such equipment and strengthen resilience against intensifying supply chain threats to the grid.

The starting point to do so is to provide industry with a holistic, end-to-end assessment of how foreign adversaries are likely to use compromised equipment to actually conduct an attack. It is (remotely) possible that opponents might seek to compromise BPS transformers so that they begin leaking oil at some pre-determined date. However, US intelligence agencies have determined that foreign adversaries are most likely to disrupt grid infrastructure and other systems in an intense crisis with the United States. That assessment has profound implications for prioritizing measures to implement the EO and developing new countermeasures to defeat supply chain-based attacks.

The *National Counterintelligence Strategy* emphasizes that adversaries are targeting supply chain vulnerabilities and conducting other pre-attack operations so that they can "exploit, disrupt and damage U.S. and allied critical infrastructure and military capabilities during a crisis."[17] In particular, the 2012 Department of Defense (DOD) *Mission Assurance Strategy* and follow-on

[16] White House, Executive Order on Securing the United States Bulk-Power System, Section 2(d)(iii).

[17] NCSC, National Counterintelligence Strategy, 3.

Defense documents emphasizes the risk that adversaries will attack the US grid and other infrastructure on which the Department depends to deploy forces to the crisis zone.[18]

A confrontation over Taiwan or some other flash point in the South China Sea exemplifies how such an attack could occur. Michèle Flournoy, former Undersecretary of Defense for Policy, warns that "Chinese military planning for taking Taiwan by force envisions early cyberattacks against the electric power grids around key military bases in the United States, to prevent the deployment of U.S. forces to the region."[19] A US-Russia crisis in the Baltics or other areas of intensifying conflict could spur similar efforts to disrupt the flow of forces to those regions as well.[20] The implication for grid resilience (including the SCRM measures envisioned in the Executive Order): protecting DCEI equipment should be a top priority for implementing the EO.

As Flournoy notes, many of the same electric systems that serve military bases "also support the surrounding civilian population, including hospitals, emergency services, and other functions critical to public safety."[21] But Russia or China may view these collateral effects as an advantage for convincing US leaders to back down in the crisis. As the *Counterintelligence Strategy* puts it, adversaries will seek to coerce "U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption."[22] More specifically, by disrupting the grid to inflict suffering on US citizens and damage the economy, opponents will seek to heighten the perceived costs of defending US allies and interests and drive US leaders to yield rather than endure further damage.[23] Protecting the critical electric infrastructure that serves facilities and functions vital for public safety and the economy should therefore constitute an additional priority for EO implementation.[24]

Of course, an attack on the grid would almost certainly be met with a devastating US response. That prospect will help deter adversaries from using compromised BPS equipment to inflict blackouts in a crisis. However, the *National Security Strategy of the United States* (2017) also emphasizes the need to "deter enemies by denial" – that is, by "convincing them that they cannot

---

[18] DOD, Mission Assurance Strategy; DOD, DoD Directive 3020.40: Mission Assurance (MA), Washington, DC: DOD, effective November 29, 2016, https://fas.org/irp/doddir/dod/d3020_40.pdf; DOD, DoD Manual 3020.40, Volume 1: Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP), Washington, DC: DOD, effective May 23, 2017, https://www.hsdl.org/?abstract&did=801336; DOD, DoD Instruction 3020.45: Mission Assurance (MA) Construct, Washington, DC: DOD, effective August 14, 2018, p. 1, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf?ver=2018-08-14-081232-450.

[19] Michèle A. Flournoy, "How to Prevent a War in Asia: The Erosion of American Deterrence Raises the Risk of Chinese Miscalculation," Foreign Policy, June 18, 2020, https://www.foreignaffairs.com/articles/united-states/2020-06-18/how-prevent-war-asia.

[20] Paul N. Stockton with John P. Paczkowski, "Strengthening Mission Assurance Against Emerging Threats Critical Gaps and Opportunities for Progress," Joint Forces Quarterly Issue 95 (4th Quarter 2019): 23, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-95/jfq-95.pdf.

[21] Flournoy, "How to Prevent a War in Asia."

[22] NCSC, National Counterintelligence Strategy, 6.

[23] For a deeper analysis of how adversaries will use cyberattacks to alter the US calculus of costs and benefits in regional crises, see: Paul Stockton, Defeating Coercive Information Operations in Future Crises, Laurel, MD: Johns Hopkins University Applied Physics Laboratory, forthcoming.

[24] The Federal Power Act identifies critical electric infrastructure as "a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters." See: 16 U.S.C. § 824o–1, Section (a)(2).

accomplish their objectives through the use of force or other forms of aggression."[25] The Strategy notes that "a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives."[26] Industry and government should implement the EO in ways explicitly designed to bolster deterrence by denial, and thereby reduce the likelihood of attacks on the grid.

Doing so will require countering threats to a wide array of critical BPS components. Many of these components have different supply chain vulnerabilities and will vary in terms of the malware or other compromises that adversaries will seek to insert. But all such equipment shares a common feature: if adversaries want to use it to coerce US behavior in a crisis, they will need to time their attacks accordingly (and perhaps also carefully target the outages they induce). That need, in turn, will likely require specialized measures to design, enable, and conduct supply chain-based attacks. Establishing a kill chain to better understand such threats could offer immense benefits for shaping EO execution and strengthening BPS resilience.

III. DEVELOPING A COMPROMISED EQUIPMENT KILL CHAIN

Beginning in the 1990s, the US Air Force and other DOD components developed the "F2T2EA" kill chain to facilitate bombing campaigns and other kinetic operations. The sequential steps in this kill chain are: *finding* the target; *fixing* its location; *tracking* and observing it; *targeting* it with a suitable weapon; *engaging* the target (i.e., conducting the attack); and *assessing* the attack's effects.[27] Researchers have since updated the F2T2EA kill chain to better understand how Russia or other adversaries might employ cyberattacks against the US. In 2011, Eric M. Hutchins, Michel J. Cloppert, and Rohan M. Amin published a pioneering study on the steps that such a kill chain would entail.[28] Michael J. Assante and Robert M. Lee subsequently built on that analysis to establish a specialized kill chain for cyberattacks on ICS in the power grid and other critical infrastructure systems. Now, leveraging insights from both those models, DOE and its public and private sector partners should develop a compromised equipment (CE) kill chain.

The benefits of doing so: once the specific steps in a kill chain have been identified, defenders can tailor countermeasures against them. The 2011 *Intelligence-Driven Computer Network Defense* study (which helped provide the basis for Lockheed Martin's Cyber Kill Chain™ model) proposed defensive courses of action for each step in the chain. Similarly, Assante and Lee use their ICS kill chain analysis to identify new opportunities for detection, remediation, and defense against threats

[25] Donald Trump, *National Security Strategy of the United States of America*, Washington, DC: The White House, December 2017, 28, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

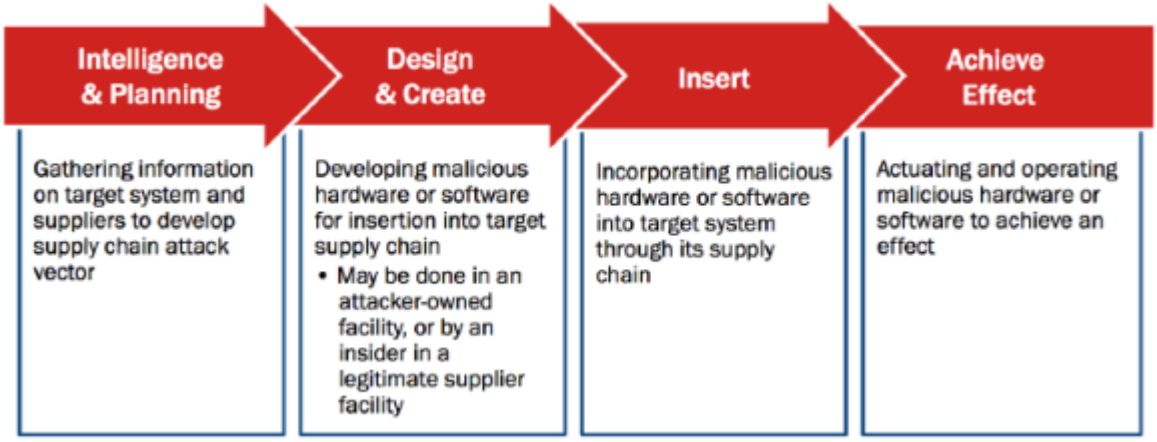
[26] Trump, *National Security Strategy*, 13. Other recent statements and strategies emphasize the importance of deterrence by denial. See, for example: US Department of State (DOS), *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats,* Washington, DC: DOS, May 31, 2018, 2, https://www.state.gov/documents/organization/282253.pdf; United States of America Cyberspace Solarium Commission, *Official Report*, Washington, DC: Cyberspace Solarium Commission, March 2020, 4, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

[27] For a detailed breakdown of these kill chain steps and their application to current Air Force doctrine for "dynamic targeting," see: United States Air Force, *Dynamic Targeting and the Tasking Process*, Montgomery, AL: Curtis E. Lemay Center for Doctrine Development and Education, last updated March 15, 2019, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-60/3-60-D17-Target-Dynamic-Task.pdf.

[28] Hutchins, Cloppert, and Amin, *Intelligence-Driven Computer Network Defense*, 4.

to the grid and other infrastructure sectors, including "active defense" and incident response.[29] An industry-government partnership aimed at developing a CE kill chain could enable the design of new countermeasures as well.

A 2017 study by the Defense Science Board's Task Force on the Cyber Supply Chain provides a starting point to support that effort. Figure 1 depicts the basic steps in the study's kill chain for inserting malware or other compromises.[30]



Many of these same steps will likely apply to efforts to corrupt BPS equipment supply chains as well.

Exploiting the Adversary's CE Kill Chain: Command and Control as an Example

Existing cyber and ICS kill chains provide a starting point to analyze US defensive options against compromised equipment-based attacks on the grid. Command and control and supporting communications links provide one such opportunity. Lockheed's cyber kill chain report notes that typically, compromised systems "must beacon outbound to an Internet controller server to establish a C2 channel," and thereby gives intruders "hands on the keyboard" access inside the target.[31] The ICS kill chain emphasizes the importance of C2 in the chain's "management and enablement" phase.[32] Assante and Lee identify a number of means by which adversaries might establish communications links to exercise these C2 functions and gain the "managed and enabled access" that will help attackers achieve their goals.[33]

Intuitively, we might expect attacks using compromised BPS equipment to have equivalent requirements for persistent C2 and supporting communications, especially if adversaries seek to

[29] Assante and Lee, The Industrial Control System Cyber Kill Chain, 20.

[30] Defense Science Board (DSB), Task Force on Cyber Supply Chain, Washington, DC: Department of Defense (DOD), February 2017, 5, https://www.hsdl.org/?abstract&did=799509.

[31] Hutchins, Cloppert, and Amin, Intelligence-Driven Computer Network Defense, 5.

[32] Assante and Lee, The Industrial Control System Cyber Kill Chain, 5.

[33] Assante and Lee, The Industrial Control System Cyber Kill Chain, 5. For an example of implanting equipment to create a communication bridge, see Stephen Hilt's PLCpwn demonstration, in which he embedded a wireless communication channel into a PLC chassis: Dale Peterson, "S4x14 Video: Stephen Hilt on PLCpwn," Digital Bond, February 3, 2014, https://dale-peterson.com/2014/02/03/s4x14-video-stephen-hilt-on-plcpwn/.

time and target their attacks for leverage in a crisis. The most direct means for adversaries to establish and exploit such C2 links is to use the sensors and communications systems already embedded in grid components. Modern transformers have multiple digital devices and sensors, including digital "tap changers" that set voltage levels, cooling system gauges and controls, and other components.[34] Adversaries might seek to compromise such devices and use them to disable or mis-operate transformers along selected DCEI power corridors.

BPS entities are very much aware of these risks and are taking aggressive measures to reduce them. Power companies typically send "expert witnesses" to transformer manufacturing plants to monitor their production and extensively test tap changers and other devices to ensure their integrity before installing the transformers on the grid.[35] Such efforts are essential for disrupting a key stage in the adversary's CE kill chain: inserting compromised digital controls and communications links to them.

Other steps in the kill chain provide additional defensive opportunities. For example, as opponents seek to maintain persistent C2 over compromised devices, and (ultimately) use this equipment to conduct attacks, such activities may entail communications and other anomalous behavior distinct from normal device operations. Such operations could open up a range of opportunities to detect compromised BPS equipment and defeat adversary attacks. The National Institute of Standards and Technology (NIST) and its industry partners have already developed voluntary technical approaches to detect anomalous behavior in industrial control systems, including adversary efforts to exploit the growing (and dangerous) opportunities for remote access of those devices.[36] Network and agent-based strategies for behavioral anomaly detection could offer especially promising applications to detect and counter C2 operations necessary for attacks using compromised equipment.[37] Many commercial network products for ICS security already provide anomaly detection functions and provide a head start for CE-related applications.[38]

---

[34] Richard Harada and Edgar Sotter, "Real-Time Remote Monitoring of Sites and Assets – Part II," EE Online, August 2018, https://electricenergyonline.com/energy/magazine/1144/article/Real-Time-Remote-Monitoring-of-Sites-and-Assets-Part-II.htm.

[35] Blake Sobczak and Peter Behr, "China and America's 400-ton electric albatross," E&E News, April 25, 2019, https://www.eenews.net/stories/1060216451/.

[36] James McCarthy et al., *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*, Gaithersburg, MD: National Institute of Standards and Technology (NIST), November 2018, 1-3, https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf.

[37] McCarthy et al., *Behavioral Anomaly Detection*, 14-16; Cheng Feng, Tingting Li, and Deeph Chana, "Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks," *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Denver, CO, 2017, 261-272, https://ieeexplore.ieee.org/document/8023128.

[38] Such commercial products include Nozomi Networks, Flowmon Networks, CyberX, and Symantec's Anomaly Detection for ICS. See, for example: Edgard Capdevielle, "ICS Anomaly Detection: Finding the Right Needle in the Relevant Electric Haystack," ICS Cyber Security Conference, November 8, 2017, https://www.icscybersecurityconference.com/ics-anomaly-detection-finding-right-needle-relevant-electric-haystack/; "ICS/SCADA Monitoring and Anomaly Detection," Flowmon Networks, May 24, 2019, https://www.flowmon.com/en/blog/ics-scada-monitoring-and-anomaly-detection; "BAD to the Bone — NIST, LOTL, and IoT/ICS Behavioral Anomaly Detection (BAD)," CyberX, May 8, 2020, https://cyberx-labs.com/blog/bad-to-the-bone-nist-lotl-and-iot-ot-behavioral-anomaly-detection-bad/. For a survey of these products, see: Carl M. Hurd and Michael V. McCarthy, *A Survey of Security Tools for the Industrial Control System Environment*, Idaho Falls, ID: June 12, 2017, https://www.osti.gov/biblio/1376870.

However, grid modernization is creating new options for adversary exploitation and greatly increase the scale and complexity of US requirements to counter them. Transformers are only one of many types of BPS equipment that have embedded sensors and two-way communications links.[39] These trends in digital substation automation and in the deployment of increasingly sophisticated protection, monitoring, and control systems are improving the efficiency of grid operations.[40] With the growing importance of distributed energy resources and variable power generation in all three US interconnections, the deployment of additional digital control devices and networks to link them will accelerate.[41]

Moreover, we should expect adversaries to seek to evade detection and minimize or avoid creating the anomalous signatures that could alert defenders to the presence or impending use of corrupted BPS products. The use of insider threats offers a prime means to do so. If adversaries can place personnel inside a BPS entity, those personnel may be able to insert and/or covertly trigger an attack using compromised equipment. Power companies have increasingly stringent programs to counter insider threats. Those initiatives will be essential to counter supply chain-based attacks, as well as intentional mis-operation of the grid and other threat vectors that insiders can employ.

Another possible adversary countermove would be to develop technologically sophisticated means of triggering attacks without detectable C2 communications. ComEd's 2019 Operation Power Play exercise featured one such option. In that exercise scenario, the attack occurred in the aftermath of devastating storms, with latent malware activating as internet outages disrupted connections to command and control servers.[42] Other options for triggering attacks based on grid conditions may exist as well, including some that may be more suitable for the timing requirements entailed in crisis operations.

Finally, and especially concerning, adversaries may seek to leapfrog steps in the kill chain by exploiting "latent vulnerabilities" that exist in BPS networks and other equipment, versus compromises that they insert. The Defense Science Board study notes that many DOD systems rely on commercial off the shelf (COTS) software and other components that may have vulnerabilities known to the attacker. These vulnerabilities can provide adversaries with a short cut to disrupt US systems.[43] The same may be true of BPS industrial control systems and other assets. The advantage of exploiting such latent vulnerabilities: rather than go through the multiple kill chain steps necessary to do design and insert compromises, adversaries can attack the grid by exploiting points of attack already embedded in the bulk power system.

---

[39] John McDonlald, "Substation Automation Basics - The Next Generation," EE Online, June 2007, https://electricenergyonline.com/energy/magazine/321/article/Substation-Automation-Basics-The-Next-Generation.htm.

[40] "Grid Modernization and the Smart Grid," DOE, n.d., https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid; McDonlald, "Substation Automation Basics.

[41] DOE, *Grid Modernization Multi-Year Program Plan*, November 2015, https://gmlc.doe.gov/sites/default/files/documents/Grid%20Mod%20Multi-year%20Program%20Plan%20-%20DRAFT.pdf; Clarion Energy Content Directors, "Digital substation initiative launched to modernize power grid infrastructure," Power Grid International, June 29, 2020, http://power-grid.com/2020/06/29/digital-substation-initiative-launched-to-modernize-power-grid-infrastructure/.

[42] "Operation Power Play," Argonne National Laboratory, n.d., https://www.anl.gov/sss/operation-power-play.

[43] DSB, *Task Force on Cyber Supply Chain*, 8-9.

However, not all BPS equipment is at equal risk of containing COTS software with exploitable vulnerabilities. Transformers will present very different risk profiles than industrial control systems, safety instrumented systems, or other BPS equipment specified by the EO.[44] Adversary kill chains and opportunities for the US to exploit them will vary by equipment type. While developing a basic CE kill chain constitutes an essential step forward for EO implementation, more nuanced, equipment-specific versions will also be necessary to support the development of cost-effective countermeasures.

Creating a Multi-Step Kill Chain Strategy

The example of C2-based countermeasures illuminates a broader requirement for EO implementation: rather than seeking to exploit one or two steps in the adversary's CE kill chain, the US needs to examine all such steps and selectively develop and implement the most cost-effective countermeasures for BPS defense. A comprehensive EO implementation strategy will also need to account for the risks posed by latent vulnerabilities.

MITRE's ATT&CK program can provide invaluable support for anticipating all such potential means of attack. That program provides an extensive, continuously updated database and model of cyber adversary behavior.[45] Such data will be vital to keep pace with adversary efforts to tailor their tactics, techniques, and procedures (TTPs) to exploit the specialized opportunities for supply chain-based attacks, including in ways very different from those associated with Black Energy, HAVEX, or other cyberattacks on foreign critical infrastructure.[46]

Another way to develop and implement a comprehensive, multi-step kill chain strategy is to draw lessons learned from DOE's Freeze Frame program. That program was structured to identify the steps that specific nations would need to take to acquire nuclear weapons, within the nuclear fuel cycle (to provide weapons-grade material) and in the weapons design, development, and production process.[47] Especially valuable, Freeze Frame provided a way to focus intelligence gathering and integrated threat reporting. Supply chain threats to the BPS pose entirely different challenges than nuclear proliferation. Nevertheless, Freeze Frame provides a model for analytic integration that could help inform the development of a comprehensive CE kill chain and anticipate adversary initiatives.

An additional model to leverage is the Consequence-driven Cyber-informed Engineering (CCE) Kill Chain. This methodology focuses on understanding adversary requirements to create major

---

[44] White House, *Executive Order on Securing the United States Bulk-Power System*, Section 4(b).

[45] Blake E. Strom et al., *MITRE ATT&CK™: Design and Philosophy*, McLean, VA: MITRE, July 2018, https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf; "ATT&CK® for Industrial Control Systems," MITRE, last edited June 3, 2020, https://collaborate.mitre.org/attackics/index.php/Main_Page; Otis Alexander, Misha Belisle, and Jacob Steele, *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*, McLean, VA: MITRE, March 2020, https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT%26CK_for_ICS_-_Philosophy_Paper.pdf.

[46] "The Evolution of Cyber Attacks on Electric Operations," Dragos, Inc., July 30, 2019, https://www.dragos.com/blog/industry-news/the-evolution-of-cyber-attacks-on-electric-operations/.

[47] DOE, *Nuclear Fuel Cycle and Weapons Development Process*, Richland, WA: Pacific Northwest National Laboratory, January 2009, http://plaza.ufl.edu/sjoden/ENU4930/Week2/Non-Prolif-FreezeFrame2009.pdf. For the application of the Freeze Frame methodology to Iran, see: Thomas E. Shea, *Assuring Effective IAEA Verification of the Iran – P5+1 Agreement*, Washington, DC: Search for Common Ground, July 2015, https://www.sfcg.org/wp-content/uploads/2015/07/Shea_Paper_Final-3.pdf.

blackouts or achieve other high consequence events.[48] In particular, the CCE Kill Chain clarifies how adversaries can target vendors and subcontractors through supply chain or human recruitment tactics in conjunction with a cyber campaign.[49] Such adversaries may insert corrupt components or software several layers into the supply chain. Opponents may also seek to co-opt insiders or have their own agents apply for critical positions at the target organization, or at one of their subcontractors or vendors. Drawing on the CCE Kill Chain's methodology for assessing (and ultimately, countering) such risks could help kick-start the development of a kill chain focused on EO implementation.

DOE's Office of Intelligence and Counterintelligence (IN) can also provide crucial support for developing a comprehensive kill chain strategy. IN and the broader US intelligence community should reinforce their existing capabilities to identify and assess potential supply chain threats to BPS equipment. They should ensure that the priority attached to intelligence collection on such threats reflects the President's determination that "the unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat" to US security.[50] As will be discussed in the final section of this report, IN and the IC should also securely share their findings with cleared BPS and vendor personnel to help provide a foundation for collaborative EO implementation.

Not all potential US exploits of the adversary's CE kill chain will be equally valuable for BPS defense. Efficient and effective implementation of the EO will require both the identification of the steps in that kill chain and a careful analysis of the costs and benefits of US measures to disrupt them. Technologically exquisite but expensive countermeasures may offer fewer benefits than more straightforward approaches – including measures to prevent the insertion of compromised equipment by scrutinizing equipment producers and their subcontractors for foreign influence, which Section IV will highlight. The US might also prioritize efforts that deprive adversaries of their most promising, high-impact targets for equipment compromise and drive them down to pursue more difficult and less cost-effective options.

Of course, foreign adversaries will attempt to anticipate US countermeasures and optimization strategies and shift their supply chain corruption efforts accordingly. The US should complicate their efforts to do so by securing sensitive SCRM plans defensive initiatives. US officials should also explore opportunities for feints and deception. Keeping adversaries guessing as to whether their equipment comprises would actually function as intended in a crisis, and not publicizing all US defensive efforts and accomplishments, could help raise adversary doubts as to whether they could achieve their goals in attacking the grid.

Beyond the Kill Chain: Emergency Operations to Limit Grid Disruptions

The final step in kill chains is typically that of triggering malicious software or hardware to launch an attack. However, once attacks are underway, significant opportunities will exist to limit their

[48] Stacey Cook and Sarah G. Freeman, *CCE Phase 3: Consequence-based Targeting*, Idaho Falls, ID: INL, May 5, 2020, 2, https://www.osti.gov/biblio/1617456.

[49] The 2014 HAVEX campaign exemplifies such TTPs. During this campaign, the adversary intercepted and altered update packages for ICS and auxiliary equipment. This effort directly targeted its victims' operations by piggybacking on the update process for non-internet facing and air-gapped machines. See: Cook and Freeman, , *CCE Phase 3: Consequence-based Targeting*, 2.

[50] White House, *Executive Order on Securing the United States Bulk-Power System*.

effects. BPS entities already have robust, well-exercised capabilities to protect and restore reliable electric service if cyberattacks occur. As these organizations partner with DOE to implement the EO, they should explore how they might apply these emergency plans and capabilities to defeat supply chain-based attacks and prevent adversaries from disrupting DCEI and achieving the other goals they seek.

Many of the emergency operations that BPS entities are prepared to conduct under their own authorities will be useful against multiple threat vectors. For example, plans for load shedding to protect system reliability can limit the disruptive effects of CE-based attacks, as well as the impacts of other manmade and natural hazards. DOE also has existing authorities that they could apply once attacks are underway. In particular, if attacks trigger the presidential declaration of a grid security emergency (GSE), the Secretary of Energy can issue GSE orders to BPS entities to protect and restore grid reliability.[51] DOE and industry are already developing and exercising "template" GSE orders for the prioritized restoration of power to critical facilities.[52] These partners should explore whether and how they might create specialized GSE orders to reduce the impact of supply chain-based attacks.

Post-attack plans and capabilities can also build on existing industry programs to provide and transport spare equipment. The SpareConnect program, for example, provides a formal mechanism for utilities to share transformers and related equipment in emergencies.[53] Industry has also established plans and coordination mechanisms for the transportation of replacement equipment. The electricity subsector established the Transformer Transportation Working Group (TTWG) to help the power companies and their partners develop plans and improve capabilities to move Large Power Transformers (LPTs) in an emergency.[54] As intelligence analysis and consequence-based risk assessments help identify especially critical BPS equipment beyond transformers, industry should consider expanding the scope of its spare equipment inventories and distribution plans, ideally in coordination with vendors. The partners will also need to counter the (very likely) possibility that adversaries will seek to compromise both stored spares and in-place equipment.

IV. DEFENSE IN DEPTH AGAINST THE INSERTION OF COMPROMISED EQUIPMENT

As EO implementation goes forward, industry and DOE should follow two very different and mutually supportive approaches to counter the insertion step in adversary CE kill chains. The first approach lies in ensuring that critical BPS equipment is not "designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a

[51] 16 U.S.C. § 824o–1, Section (a)(7)(A) and Section (b). For an analysis of how the Secretary might employ GSE orders to protect and restore grid reliability, and the prerequisites for doing so, see: Paul Stockton, *Resilience for Grid Security* Emergencies*: Opportunities for Industry-Government Collaboration*, Laurel, MD: John Hopkins University Applied Physics Laboratory (JHU-APL), 2018, https://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf.

[52] NERC, *GridEx V: Lessons Learned Report*, Atlanta, GA: NERC, March 2020, 3, https://www.nerc.com/pa/CI/CIPOutreach/GridEX/TLP%20WHITE%20GridEx%20V%20Lessons%20Learned%20MAR20.pdf.

[53] "About," SpareConnect, n.d., http://spareconnect.org/about/.

[54] DOE, *Strategic Transformer Reserve: Report to Congress*, Washington, DC: DOE, March 2017, 12, https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf.

foreign adversary."[55] BPS entities are already using mandatory standards and voluntary frameworks and best practices to help achieve this goal, thereby reducing the risks of supply chain corruption.

Adversaries will almost certainly seek to evade such efforts by covertly penetrating subcontractors or taking other measures to defeat industry-government oversight of the processes by which equipment is produced. To supplement these process-oriented SCRM initiatives, it will be necessary to not only continually strengthen them, but also to adopt a second approach: testing and evaluation of equipment that poses the greatest potential risks to BPS reliability. DOE and industry should systematically integrate and guide the expansion of both sets of initiatives in implementing the EO.

Scrutinizing Vendors and Strengthening SCRM Processes

NERC has established (and FERC has approved) a series of mandatory standards to reduce BPS supply chain risks. CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments).[56] Especially significant for achieving the EO's goals, CIP-013-1 is designed to "mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems."[57]

NERC has also issued industry-wide alerts in 2017, 2019, and 2020 on "Supply Chain Risk."[58] While these alerts are not publicly available, NERC CEO Jim Robb spoke about the 2019 alert, which sought to identify Chinese equipment in BPS systems and associated mitigation strategies for potential supply chain risks.[59] In addition, NERC has extensive and growing supply chain risk mitigation programs, including a working group for supply chain issues.[60] All of these initiatives and collaborative relationships are of foundational importance for implementing the EO.

To supplement NERC's mandatory standards, the electric industry is also advancing voluntary SCRM initiatives. The NATF is already playing a key role in coordinating supply chain cybersecurity initiatives for electric industry organizations, vendors, and third-party assessors, and could serve in a coordination role for EO implementation. Working beyond its membership, NATF has created the Industry Organizations Team for cross-industry, cross-sector (gas), and cross-border (Canada) collaboration.[61] As part of that effort and in partnership with additional industry

[55] White House, *Executive Order on Securing the United States Bulk-Power System*, Section 1(a)(i).

[56] Federal Energy Regulatory Commission (FERC), *Supply Chain Risk Management Reliability Standards* (Docket No. RM17-13-000), Federal Register Vol. 83, No. 208 (October 26, 2018): 53,992.

[57] North American Electric Reliability Corporation, *CIP-013-1 – Cyber Security – Supply Chain Risk Management*, July 2017, 3, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

[58] "Alerts," NERC, accessed July 30, 2020, https://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx.

[59] Molly Christian, "NERC to ask utilities to inventory reliance on Chinese technology," S&P Global, July 12, 2019, https://www.spglobal.com/marketintelligence/en/news-insights/trending/peha_2jR2jCRPAdm2DIX-w2.

[60] "Supply Chain Risk Mitigation Program," NERC, n.d., https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx; "Supply Chain Working Group (SCWG)," NERC, https://www.nerc.com/comm/CIPC/Pages/SCWG.aspx.

[61] North American Transmission Forum (NATF), *North American Transmission Forum External Newsletter*, Washington, DC: NATF, April 2020, 4, https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---april-2020.pdf.

organizations, NATF members and the Industry Organizations Team have developed the *Supplier Cyber Security Assessment Model,* the *NATF Cyber Security Criteria for Suppliers,* and the *Energy Sector Supply Chain Risk Questionnaire.*[62] The model, criteria, and questionnaire aim to create a streamlined and industry-accepted approach to obtain verified critical information for evaluating suppliers' cybersecurity practices and conducting risk assessments.[63] The NATF's risk assessment initiatives are the most mature in the electric industry to date and provide a critical foundation for future supplier assessment efforts. NATF, with its Industry Organization Team, is uniquely positioned to rapidly advance solutions by recognizing and uniting accomplishments from all industry organizations, suppliers, third-party assessors, and vendors providing solutions for industry, government agencies, and regulators.

Other industry and government organizations are facilitating voluntary SCRM efforts as well. Especially important, NIST and its industry partners have developed a Cyber Supply Chain Risk Management program, which supports its users in "identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains."[64] The program covers a system's entire life cycle (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise products and services, including those employed in the BPS.[65]

Testing and Evaluation

In addition to better monitoring subcontractors and making other SCRM process-oriented improvements, it will be necessary to test and evaluate products that are critical to grid reliability. T&E programs can help mitigate the risk that adversaries will be able to maneuver around process-oriented supply chain standards and enforcement measures. Adversaries will no doubt seek to do so. NERC warns that:

> Certain vendors can introduce their goods into locations of strategic interest through insurmountable competitiveness on cost likely subsidized by the host vendor's host nation. Deliberately opaque and convoluted networks of largely unknown resellers and brokers with bids deliberately crafted to exploit the acquisition rules of the target customer are sometimes used to mask these activities. For power system and telecommunications facilities, turnkey engineering-procurement-construction management contracts are an enduring risk throughout the entire lifecycle of the infrastructure, increasing exposure to the threat. In the most extreme cases, simply acquiring the target organization or a connected entity is a feasible option for the most well-resourced adversaries. While legal and regulatory controls in the United States and Canada may prevent direct use of this

[62] "Supply Chain Cyber Security Industry Coordination," North American Transmission Forum NATF, n.d., https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[63] NATF, *Supplier Cyber Security Assessment Model*, Charlotte, NC: NATF, January 31, 2020, 5, https://www.natf.net/docs/natf/documents/resources/supply-chain/supplier-cyber-security-assessment-model.pdf.

[64] "Cyber Supply Chain Risk Management," NIST, last updated June 22, 2020, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

[65] "Cyber Supply Chain Risk Management," NIST.

tactic, these defenses would not necessarily preclude the adversary from locking down strategic portions of a broader value chain.[66]

We should also expect adversaries to exploit simplistic, "Buy American" strategies to defend the grid. This is especially true with regard to identifying pre-approved vendors. The EO states that the Secretary of Energy may "establish and publish criteria for recognizing particular equipment and particular vendors in the bulk-power system market as pre-qualified" for purchase by BPS entities.[67] Establishing such criteria and listing approved equipment could significantly assist BPS procurement activities. However, as DOE does so, it will be vital to account for the risk of insider threats and other TTPs for the insertion of compromises in such pre-approved equipment, even if SCRM process controls are in place to ensure that no subcomponents are produced by vendors on the territory of (or influenced by) foreign adversaries. Grid defense will also require sustained focus on the risk that adversaries will exploit latent vulnerabilities in grid software and systems, even when that software is sold by US vendors.

Programs to test and evaluate critical BPS equipment can back-stop process-oriented SCRM improvements and complicate adversary efforts to prepare for attacks on the grid. The CyTRICS program is the most significant DOE-sponsored initiative currently underway to develop such T&E capabilities. Alexander Gates, Senior Advisor in DOE's Office of Policy for Cybersecurity, Energy Security, and Emergency Response (CESER) testified to Congress that CyTRICS provides "a central capability for the DOE's efforts to increase energy sector cybersecurity and reliability through the testing and enumeration of critical components to identify and mitigate embedded cyber vulnerabilities across the energy sector." He also noted that DOE's "analysis of test results will identify systemic and supply chain risks and vulnerabilities to the sector by correlating collected test data and enriching it with other pertinent data sources and methods."[68]

NERC, FERC, and their industry partners have also identified a number of ways in which programs developed to test selected telecommunications equipment (including systems used by BPS entities) could be leveraged for a broader array of products.[69] In addition, the Johns Hopkins University Applied Physics Laboratory, the Cybersecurity Manufacturing Innovation Institute, and other EO implementation partners are developing technologies to isolate suspect components and mitigate the risks they pose to system operation.[70]

---

[66] NERC, *2020 State of Reliability: An Assessment of 2019 Bulk Power System Performance*, Atlanta, GA: NERC, July 2020, 78, https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf.

[67] White House, *Executive Order on Securing the United States Bulk-Power System*, Section 1(d).

[68] Alexander Gates, testimony before the United States Senate Committee on Energy and Natural Resources, August 5, 2020, 3, https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=FED4D625-905A-4AB9-9231-BCE8DCE45155.

[69] NERC and the Federal Energy Regulatory Commission (FERC), *Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller*, Atlanta, GA: NERC, July 31, 2020, https://www.nerc.com/pa/comp/CAOneStopShop/Joint%20Staff%20White%20Paper%20on%20Supply%20Chain_07312020.pdf.

[70] For example, DHS and the US Coast Guard have tasked the Applied Physics Laboratory to demonstrate the use of a virtualized programmable logic controller (vPLC) to enable an ICS to automatically detect, react, and reconfigure itself for resilience. DOE also funded the University of Texas at San Antonio (UTSA) to establish the Cyber Manufacturing Innovation Institute. See: "U.S. Department of Energy selects UTSA to lead Cybersecurity Manufacturing Innovation Institute," UTSA Today, May 27, 2020, https://www.utsa.edu/today/2020/05/story/DOE_selects_UTSA_CyManII.html.

T&E programs can also backstop process-oriented SCRM efforts at the system level. While testing transformers and other pieces of vital BPS equipment must be a near-term priority, it will also be important to test representative systems. Once we clarify likely adversary objectives (including the disruption of force deployments in regional crises) and have established a kill chain for attacks that employ compromised equipment, DOE and its partners should explore ways to assess the system-wide effects of such attacks using modeling and simulations and test ranges. Testing at that system level may enable the development of new options to defend the grid.

However, implementing the EO will require industry and government to reach consensus on two major programmatic challenges. The first is that of determining which equipment is most important to test. So many products are essential to grid reliability that it will be essential to prioritize such testing, especially for potentially compromised equipment that may already be installed in DCEI. The EO lists over a dozen types of equipment that will be part of the implementation process to secure the BPS, including: reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacity voltage transformers, protective relaying, metering equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems.[71] Moreover, each of these types of equipment have multiple suppliers, with each supplier typically providing multiple versions of their products to BPS customers.

Industry and government might adapt a number of existing methodologies to establish priorities within this diverse array of equipment. One option is to employ Consequence-driven Cyber-informed Engineering to determine which types of compromised equipment would allow adversaries to best achieve their objectives – for example, disrupting electric service to the multiple Defense installations and supporting infrastructure necessary for deploying US forces to the South China Sea or other potential conflict zones.[72] Mission dependency modeling and other methodologies could also help target T&E assessments.[73] All such prioritization efforts would benefit from analytic support on threats to BPS equipment from DOE IN and its intelligence community partners.

The second major challenge for testing and evaluation lies in scaling up existing T&E programs. Even with harsh prioritization, the number and diversity of BPS components that need testing are far greater than current US testing capabilities provided by national laboratories, private companies, and BPS entities themselves. DOE should collaborate with these partners to forge a strategy (and provide the necessary funding) to expand and sustain US T&E capabilities.

That strategy will need to address the significant constraints faced by CyTRICS and other existing T&E efforts. Gates notes that "DOE has signed multiple agreements with energy sector partners to grow the CyTRICS™ program from a proof of concept to a robust supply chain cybersecurity

[71] White House, *Executive Order on Securing the United States Bulk-Power System*, Section 4(b).

[72] Sarah G. Freeman, Nathan Hill Johnson, and Curtis P. St. Michel, *CCE Phase 1: Consequence Prioritization*, Idaho Falls, ID: Idaho National Laboratory, May 5, 2020, https://www.osti.gov/biblio/1617458.

[73] See, for example, the JHU-APL "Dagger" mission modeling and real-time assessment tool. JHU-APL, *2014 Annual Report*, Laurel, MD: JHU-APL, 2014, 14, https://www.jhuapl.edu/Content/documents/2014_Annual_Report.pdf.

program for the sector," and that DOE "will continue collaborating with other Federal partners, the DOE Labs, and industry to identify key energy sector industrial control systems components and apply a targeted, collaborative approach to these efforts."[74] Nevertheless, these programs can only ramp up if vendors, BPS entities, DOE, and private security testing companies increase the availability of priority BPS equipment and data to enable that analysis. Doing so will require these partners to resolve a number of thorny issues. Chief among them:

- Vendor participation. To encourage vendors to share information and collaborate in the security testing of their equipment, it will likely be necessary to establish specialized liability protections and mechanisms to limit the distribution of sensitive data (including test results).

- Intellectual property. New arrangements may also be necessary to protect the intellectual property developed for BPS equipment subcomponent analysis. A model for such protections is provided in the FY2020 National Defense Authorization Act (NDAA), Section 5726 of which establishes a pilot program for testing and provides both liability protection and exemption from disclosure of discovered test results for participating covered entities.[75]

To enable progress on all these issues, DOE and its partners will need an organizational framework for sustained dialog and consensus-building. The section that follows recommends options for establishing such a framework to enable progress on T&E and the many other efforts necessary to achieve the EO's goals.

V. STRENGTHENING UNITY OF EFFORT FOR EO IMPLEMENTATION

A number of existing industry organizations already have SCRM initiatives underway. However, given the diversity of stakeholders who will need to collaborate to achieve the EO's goals, a dedicated, sustainable body will be necessary to coordinate and align their efforts for mutual support. Previous sections of this report highlighted the major SCRM initiatives already underway by the NATF, NERC, and other industry organizations. All of these partners will be vital for establishing a coordinating body – ideally, by building on existing organizations, rather than incurring the additional time and expense required to establish a new one. Integrating other organizations will also be vital for implementing the EO.

E-ISAC. The Center serves as the "the primary security communications channel for the electric industry."[76] As such, it will need to play major roles in sharing data on compromised equipment, coordinating with DOE to assess threats, and supporting response operations if CE-based attacks occur.

FERC. As noted above, FERC directed NERC to develop SCRM reliability standards in July 2016 and in subsequent years.[77] In addition, FERC will play another vital role in EO implementation:

---

[74] Gates, testimony before the United States Senate Committee on Energy and Natural Resources, 3.

[75] United States Congress, *S. 1790 - National Defense Authorization Act for Fiscal Year 2020*, 116th Congress, 982, https://www.govinfo.gov/content/pkg/BILLS-116s1790enr/pdf/BILLS-116s1790enr.pdf.

[76] "Electricity Information Sharing and Analysis Center," NERC, n.d., https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

[77] "FERC Directs Development of Standards for Supply Chain Cyber Controls," *Federal Energy Regulatory Commission*, July 21, 2016, https://www.ferc.gov/media/news-releases/2016/2016-3/07-21-16-E-

that of enabling cost recovery for utilities purchasing safer equipment. Complying with the Order will almost certainly require BPS entities to purchase equipment that is more costly than the low-priced products that China manufactures to penetrate US markets (and, potentially, prepare the US grid for attack). However, the Order provides no details on how companies will recover the higher costs incurred by purchasing safer equipment. FERC will play a leading role in developing mechanisms for them to do so.

FERC's *Cybersecurity Incentives Policy Whitepaper* (June 2020) examines possible financial incentives for BPS entities to strengthen the cybersecurity of their systems and options to identify investments that would be eligible for such incentives, above and beyond the measures necessary to comply with NERC's Critical Infrastructure Protection reliability standards.[78] As FERC further refines these options with industry input, cost recovery for purchasing safer equipment should be a prime focus. The same is true of other potential implementation costs, including the requirement to replace compromised in-service equipment.

The National Association of Regulatory Utility Commissioners (NARUC). While the EO applies only to BPS entities and their electric systems, adversaries may also target the distribution-level systems regulated by State public service commissioners. Adversaries are especially likely to compromise critical distribution system equipment if it helps provide the "last mile" of connectivity between BPS transmission lines and substations and defense installations and other national security facilities. Indeed, as EO implementation measures make BPS infrastructure increasingly secure, distribution systems could become all the more lucrative targets unless their defenses against supply chain-based attacks improve as well.

NARUC has commissioned research that examines supply chain threats and has convened panels on associated risks and mitigations.[79] NARUC has also analyzed how to establish guidelines for assessing wither proposed investments in cybersecurity are "reasonable, prudent, and effective." But such efforts focus primarily on helping determine whether a given investment provides sufficient economic benefits to justify their costs, expressed as the "value of lost load" that a cyber-induced blackout would entail.[80] That approach is necessary but not sufficient. Adversaries will attack the grid not only to inflict economic costs, but also to disrupt the flow of power to the specific defense installations necessary for the US to prevail in a crisis. Regulators and distribution utilities need a means of assessing the value of buying safer grid equipment for *national security*, versus for civilian customers.

8.asp#.WQC2DGnysuU; Federal Energy Regulatory Commission, *Supply Chain Risk Management Reliability Standards* (Docket No. RM17-13-000), 162 FERC ¶ 61,044, January 18, 2018, p. 5, https://cms.ferc.gov/sites/default/files/whats-new/comm-meet/2018/011818/E-2.pdf.

[78] FERC, *Cybersecurity Incentives Policy White Paper*, Washington, DC: FERC, June 2020, 14-21, https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf.

[79] See, for example: National Association of Regulatory Utility Commissioners (NARUC), *Cybersecurity Preparedness Evaluation Tool*, Washington, DC: NARUC, June 2019, 9, https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0; "Agenda-At-A-Glance," NARUC, July 2020, https://www.naruc.org/meetings-and-events/naruc-summer-policy-summits/2020-summer-policy-summit/agenda/.

[80] National Association of Regulatory Utility Commissioners (NARUC), *Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators*, Washington, DC: United States Agency for International Development, May 2020, 22-24, https://pubs.naruc.org/pub.cfm?id=9865ECB8-155D-0A36-311A-9FEFE6DBD077.

NARUC can also help the EO implementation process by offering crucial perspectives on who should pay for such national security benefits. NARUC notes that "Public Service Commissions must balance utility companies' ability to earn a profit with the public's right to receive services at reasonable rates."[81] The EO raises a broader question: if distribution-level electric systems need to pay more for safer equipment and help defeat threats from China and other foreign adversaries, is that a burden that ratepayers should bear through their electricity bills? Or is some other funding mechanism (including dedicated Federal funding) more appropriate for achieving national security objectives? NARUC can provide invaluable perspectives to help build consensus on these funding and equity issues.

Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and ONG-Information Sharing and Analysis Center (ONG-ISAC). The EO exclusively focuses equipment for the BPS. However, strengthening the resilience of electric service to critical defense installations will require sustained progress in SCRM for the oil and natural gas subsector as well. Natural gas fuels much of the electric power generation in the US.[82] Adversaries are aware of the grid's reliance on ONG infrastructure and may attack natural gas transmission systems as an indirect way of disrupting DCEI. Threats to those systems are rapidly intensifying.[83] Accordingly, as DOE and its partners implement the EO, voluntary collaboration with the ONG subsector will be essential.

DOE's North American Energy Resilience Model (NAERM) provides a basis for assessing gas-electric interdependencies and a starting point to advance sector-wide SCRM initiatives. The NAERM is structured to support incident response by improving threat identification, and providing real-time situational awareness and modeling to inform operational decision-making.[84] The NAERM will also benefit long-term planning by using its advanced modeling to identify potential infrastructure investments that will be particularly effective in improving system-wide resilience. DOE should consider how these initiatives might encompass supply chain-based threats to critical gas-electric system nodes.

---

[81] "Reasonable Rates," NARUC, n.d., https://www.naruc.org/servingthepublicinterest/about/rates/.

[82] At 38.4%, natural gas-fired generation accounted for the largest share among generation sources. See: "What is U.S. electricity generation by energy source?," US Energy Information Administration, 2020, https://www.eia.gov/tools/faqs/faq.php?id=427&t=3. This reliance on natural gas for power generation is particularly acute in New England, California, the Mid-Atlantic, and a handful of other US regions. NERC notes that some areas within North America depend natural gas to meet over 60 percent of peak demand generation. See: NERC, *2018 Long-Term Reliability Assessment*, Atlanta, GA: NERC, December 2018, 7, https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2018_12202018.pdf; NERC, *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System*, Atlanta, GA: NERC, November 2017, *vii*, https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SPOD_11142017_Final.pdf.

[83] Adversaries are also targeting equipment manufacturers, and third-party vendors to compromise ONG systems. See: Dragos, *Global Oil and Gas Cyber Threat Perspective: Assessing the Threats, Risks, and Activity Groups Affecting the Global Oil and Gas Industry,* Hanover, MD: Dragos, August 2019, 1, https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf

[84] Bruce Walker, "Keeping the Nation's Critical Energy Infrastructure Secure and Resilient Requires a Strong STEM Workforce," Department of Energy, April 5, 2019, https://www.energy.gov/articles/keeping-nation-s-critical-energy-infrastructure-secure-and-resilient-requires-strong-stem.

Ongoing industry collaboration provides an additional basis for progress. The ESCC is already working with the ONG SCC to promote cross-sector coordination.[85] However, threats and mitigation options involving critical equipment pose uniquely promising opportunities for collaboration. Many of the same industrial components in BPS supply chains that are at risk of corruption have similar counterparts in natural gas transmission systems. While some ICS components are specific to an industry's processes and operations, a vendor will often use similar firmware, software, and sub-components (i.e. microprocessors) in all of its products. Major vendors, for example, may have a specific software or application suite for ONG-specific needs.[86] However, control systems are extremely similar across sectors, and are applied in nearly every sector using similar or common configurations.[87] This commonality can be useful for protecting ICS, but also means that an adversary that has successfully compromised the supply chain can execute attacks on multiple systems without investing significant resources in understanding complex differences between different sectors' ICS. Coordinated gas-electric progress on equipment security is not only critical for protecting DCEI resilience, but also offers a much more efficient approach than pursing separate subsector initiatives.

In addition to the ONG SCC, it may be helpful to incorporate the ONG subsector's E-ISAC equivalent: the ONG-ISAC. This ISAC "serves as a central point of coordination and communication to aid in the protection of … the ONG industry, through the analysis and sharing of trusted and timely cyber threat information."[88]

Organizing for Unity of Effort: Options and Functional Requirements

A variety of options exist for structuring the voluntary coordinating body to achieve that goal. It could be placed within the ESCC, the NATF or some other existing organization that has already established deep and effective ties with multiple SCRM partners (including vendors). In contrast, progress towards ensuring sustained and integrated Federal participation in such a body remains nascent. The Task Force structure envisioned in the EO provides a starting point to organize for such collaboration – potentially over a far broader range of topics that those specified by the Order.

The structure and governance of this voluntary coordinating body should also reflect its basic functions. One crucial function should be to build on existing mechanisms under the E-ISAC and DOE to facilitate the sharing of SCRM data, based on need to know and as permitted by anti-trust regulations. As permitted by those regulations and antitrust law, the organization might also help

[85] Oil and Natural Gas Sector Coordinating Council (ONG SCC), *About the ONG SCC*, Washington, DC: ONG SCC, April 2019, 1, http://ongsubsector.com/documents/ONG-SCC-Brochure_06112019.pdf.

[86] Schneider's gas suite, for example, offers "gas day operations, real-time gas, gas measurement and analysis; liquids suite: liquids management systems; and pipeline energy management suite," and more. See: "What the oil and gas industry needs from SCADA," Oil & Gas Engineering, February 11, 2017, https://www.oilandgaseng.com/articles/what-the-oil-and-gas-industry-needs-from-scada/.

[87] Eric Cosman, "Is ICS Cybersecurity Common Across Sectors?," ARC Advisory Group, June 22, 2017, https://www.arcweb.com/blog/ics-cybersecurity-common-across-sectors.

[88] "ONG-ISAC Mission," ONG-ISAC, n.d. https://ongisac.org/.

partners coordinate on procurement strategies and purchasing decisions, ideally in ways that provide powerful, consistent, market-based incentives for vendors to produce safer products.[89]

However, the limited number of clearances available to industry may impede such sharing. That is especially true for Top Secret/Sensitive Compartmented Information (TS/SCI) clearances (and their DOE equivalents) that will be necessary for access to potentially crucial data for EO implementation. Industry leaders have urged DOE to streamline and ramp up the processing of clearances for their employees.[90] Given the imperative to protect classified data on supply chain threats, one approach might be for DOE to further prioritize the clearance process for senior leaders of BPS entities so they can better guide SCRM efforts for their systems. Operators within those entities could then execute risk reduction measures without the need for access to classified data.

The collaborative body might also facilitate operational coordination between DOE and BPS entities if supply chain-based attacks on the grid were imminent or underway. One possibility: as noted in Section III's analysis of kill chains, adversaries will likely need to communicate with their compromised equipment to prepare for or execute grid attacks during a crisis. Their efforts to send and receive C2-related data could provide a range of possible US countermeasures.

However, real-time, two-way intelligence sharing between BPS entities and the government may be necessary to facilitate such defensive operations. The Cybersecurity Risk Information Program managed by the E-ISAC is aimed at establishing a public-private data sharing and analysis platform that facilitates the timely, bi-directional sharing of unclassified and classified threat information among energy sector stakeholders.[91] Additional foundations for progress:

- *The Pathfinder Initiative.* DOD, DOE, and DHS are conducting Pathfinder to "advance information sharing, improve training and education to understand systemic risks, and develop joint operational preparedness and response activities to cybersecurity threats" to the energy sector.[92] The initiative will "strengthen interagency collaboration on preventing and responding to the constantly evolving cyber threats" to critical energy sector infrastructure in the US.[93]

- *The Cyber Analytics Tools and Techniques (CATT) 2.0™ platform.* CATT 2.0 is developing a new approach to information sharing and analysis that relies upon data from multiple sensor programs. In particular, CATT 2.0 "seeks to create a platform where data gleaned

[89] Paul Stockton, "Securing Critical Supply Chains: Strategic Opportunities for the Cyber Product International Certification (CPIC™) Initiative," *Cyber, Intelligence, and Security* Volume 2, No. 2 (September 2018): https://www.inss.org.il/wp-content/uploads/2018/10/paul.pdf.

[90] Jack Fitzpatrick, "As DOE Prepares for Cyberattacks, Energy Industry Wants More Clearances," Morning Consult, April 4, 2017, https://morningconsult.com/2017/04/04/doe-prepares-cyberattacks-energy-industry-wants-clearances/.

[91] DOE, *Cybersecurity Risk Information Sharing Program (CRISP)*, Washington, DC: DOE, September 2018, https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf.

[92] "U.S. Department of Energy, U.S. Department of Homeland Security, and U.S. Department of Defense Announce Pathfinder Initiative to Protect U.S. Energy Critical Infrastructure," DOE, February 3, 2020, https://www.energy.gov/articles/us-department-energy-us-department-homeland-security-and-us-department-defense-announce.

[93] "Pathfinder Initiative to Protect U.S. Energy Critical Infrastructure," DOE.

from a variety of sensors on energy company systems can examine threats and events on information technology and operational technology systems."[94]

- *The Structured Threat Intelligence Graph (STIG).* STIG, a tool for "creating, editing, querying, analyzing and visualizing threat intelligence," provides a further example.[95] STIG was developed by INL and Southern California Edison (SCE) under the California Energy Systems for the 21st Century (CES-21) program as an open source platform to help provide "a repeatable and sharable platform for structured threat information."[96]

- *Hunt and Incident Response Team (HIRT).* DHS' National Cybersecurity and Communications Integration Center (NCCIC) operates the HIRT, which provides "incident response, management and coordination activities for cyber incidents occurring in the critical infrastructure sectors."[97] As part of operational collaboration, DHS can deploy these teams to "identify and contain adversary activity and develop mitigation plans for removal and remediation of root cause" if attacks are imminent or underway.[98]

Going forward, these and other ongoing programs should adopt a special focus on defeating CE-induced grid disruption and account for the risk that adversaries will attempt to compromise DOE-industry information sharing networks as well as BPS equipment.

VI. CONCLUSION

The electricity subsector, DOE, and their partners have a diverse and impressive array of initiatives underway to reduce supply chain risks to the bulk power system. What is missing is an overarching strategy to integrate and prioritize their efforts to achieve the goals of the Executive Order 13920.

That strategy should be grounded on the national security context of threats to the grid. It is conceivable that foreign adversaries will compromise BPS transformers so they begin leaking oil at some random date in the future, or corrupt protective relays so they fail as soon as US power companies install them. However, based on findings from the *National Counterintelligence Strategy* and other US intelligence community reports, it is far more likely that opponents will launch CE-based attacks on the grid to coerce US behavior in a regional crisis and disrupt the flow of US forces to the crisis zone. The need to time such attacks will create distinctive adversary requirements for compromising and mis-operating BPS equipment.

Developing a compromised equipment kill chain will help identify these requirements and US options to exploit them. For example, if adversaries want the ability time their attacks for leverage

---

[94] Edison Electric Institute (EEI), *National Security Efforts in the Electric Power Sector*, Washington, DC: EEI, August 2019, 4, https://www.eei.org/issuesandpolicy/Documents/national_security_efforts_in_the_electric_power_sector.pdf.

[95] INL, "STIG – Structured Threat Intelligence Graph," GitHub, n.d., https://github.com/idaholab/STIG.

[96] INL, "STIG – Structured Threat Intelligence Graph"; Peter Behr, "DOE, utilities seek the ultimate shield against hackers," E&E News, May 31, 2019, https://www.eenews.net/stories/1060437361. CES-21 is funded by the California Public Utility Commission (CPUC), which is funding the research and development of numerous capabilities to address threats to California's energy systems. See: "Energy Research, Development & Deployment," CPUC, n.d., https://www.cpuc.ca.gov/energyrdd/.

[97] "Detection and Prevention," Cyber and Infrastructure Security Agency (CISA), last updated April 23, 2019, https://www.cisa.gov/detection-and-prevention.

[98] "Detection and Prevention," CISA.

in crises, they will likely require persistent command and control and supporting communications links with their compromised components. Any such requirement could create a wealth of opportunities to detect and counter the use of that equipment. However, we need to scrutinize every step of the adversary's kill CE chain that the US could exploit, and pursue only those countermeasures that offer the most cost-effective means of disrupting supply chain threats.

One especially promising step for exploitation lies in adversary efforts to insert compromises into US equipment. The electric industry and its partners should continue to strengthen their already robust efforts to identify vendors and subcontractors under the influence of foreign adversaries and implement mandatory standards and voluntary best practices for supply chain risk management. Yet, testing and evaluation programs will be essential to backstop those efforts. Developing an action plan to grow T&E capabilities and fund them for the long haul must be a central focus of EO implementation planning.

To create that T&E plan, as well as advance all the other initiatives cited in this analysis, input from vendors, BPS customers, and a variety of other public and private sector partners will be required. Building on existing industry coordination mechanisms and organizations can help DOE establish the collaborative body that will be necessary to integrate EO activities and enable public-private unity of effort to achieve the Order's goals.