FINITE STATE

Charles Kosak
Office of Electricity Transmission Permitting and Technical, Assistance Division
US Department of Energy,
1000 Independence Avenue, SW.
Washington, DC 20585

Via email to: *bulkpowersystemEO@hq.doe.gov*

Re: Finite State Response to Depart of Energy Request for Information - Executive Order 13920 (Securing the United States Bulk-Power System) Docket No. DOE-HQ-2020-0028

Dear Mr. Kosak,

On behalf of Finite State, we are pleased to provide these comments in support of the Department of Energy (DOE) recent Request for Information (RFI) relating to the May 1, 2020 Executive Order 13920, *Securing the United States Bulk-Power System* (E.O.). Securing our nation's critical infrastructure is imperative for us all and at the core of Finite State business operations. As a solutions provider[1] that focuses on helping organizations mitigate supply chain security risk by automating the risk assessment process and providing continuous screening of device firmware and software for threats, we are fully invested in the objectives and goals of this E.O.

Supply chain security is a complex challenge across many industry sectors and for all critical infrastructure, including the Bulk Power System (BPS). Our clients are focused on holistic approaches that leverage defense-in-depth solutions that ensure risks are considered from vendor analysis and purchase, to production and throughout the life of a product. We work to support these objectives with an emphasis on providing resources that recognize the need to be able to mitigate supply chain risks of all kinds, even where those risks may be higher with some vendors or products. This allows organizations the ability to design effective security programs while ensuring access to products and vendors to maximize operational capabilities, especially for unique operational activities where there may not be sufficient choice to exclude products or vendors.

Ultimately, our position is that, in a world dominated by global supply chains, the best approach is to evolve away from a vendor trust-based model, which prioritizes lightweight assessment and self reporting of vendor processes and provenance, to a more robust and

[1] Finite State partners with both device manufacturers and asset owners to provide automated embedded device security assessments including firmware analysis to provide software and hardware bill of materials, provenance and more. To date, Finite State has processed over 300,000 firmware images.

comprehensive approach, where every device and software application being placed within the BPS networks is being screened continuously for real threats and vulnerabilities. This approach provides a ground truth risk assessment of the actual devices and software and enables instant, retroactive analysis when new supply chain vulnerabilities and threats are identified. The feasibility of this approach has been proven by Finite State in the Huawei Supply Chain Assessment released in June 2019, which analyzed more than 9,900 firmware for Huawei enterprise network equipment.[2]

We encourage DOE to implement this E.O. balancing the critical security interest objectives against the practical operating realities for many organizations and understanding that there are a variety of solutions and tools that would allow for this possibility. We provide the below comments from that perspective and have limited our response to questions where we have information that may be useful.

Thank you, we appreciate the opportunity to respond and support the industry and DOE long-term goals for supply chain security.

Matt Wyckhouse
CEO

[2] https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf

FINITE STATE

Finite State Response to DOE RFI on Executive Order 13920

(A-1) Do energy sector asset owners and/or vendors conduct enterprise risk assessments, including a cyber maturity model evaluation on a periodic basis? Provide an explanation or description of an assessment program if it addresses the mitigation of risks associated with FOCI with respect to foreign adversaries (see https://www.dcsa.mil/mc/ctp/foci/).Start Printed Page 41025

In our experience, energy sector asset owners and vendors do conduct periodic risk assessments. Examples of common approaches include the use of vendor surveys, periodic Cyber Vulnerability Assessments (CVAs) and traditional penetration tests. These tend to be "point in time" exercises, however, and have a limited scope capability, the results of which may not fully reveal the risks and vulnerabilities within their devices. Leveraging only these measures may leave gaps in the ability to generate software provenance, which could result in unidentified risks and weaker security.

Additionally, one of the biggest challenges in implementing supply chain security is the ability to inventory the universe of assets, components and thus, risks. Where entities are able to accurately produce an inventory of their assets and run automated product assessments against all of these assets—including firmware analysis—to verify that the information being sent by the vendor is correct, they will be much better positioned to define mitigation actions and reduce risks with devices on their network.

When working with company teams and vendors, we typically recommend they run firmware analysis against all of their final firmware images in order to truly understand all the software components and libraries in their devices, which vendors those components are tied to, and the country of origin associated with those vendors. This will provide a much more accurate picture of potential risks lying within their devices. This knowledge will empower an ability to apply pressure upstream to their suppliers, thus driving through the various tiers, and allow them to define action to mitigate vulnerabilities tied to those software components.

(A-2) Do energy sector asset owners and/or vendors identify, evaluate, and/or mitigate the following:

a. FOCI with respect to foreign adversaries with respect to access to company and utility data, product development, and source code (including research partnerships)

b. potential supply chain risks from sub-tier suppliers, recognizing that some sub-tier supply chain manufacturers could have FOCI with respect to foreign adversaries

Supply chains are complex and include a wide range of vendors who introduce risk from a variety of sources, including third party and open source code and libraries which may contain critical vulnerabilities. The reality is that *every* device, software application, and vendor bring with it some level of FOCI risk. We live in a world that is fueled by global supply chains and open source software that is built by global, distributed teams of engineers. Even device manufacturers who do not contract with foreign vendors may have the components of tier 2, 3 or more removed suppliers embedded within their software due to the complexity of the typical software supply chain.

The best government led initiatives in this area are those that request a software bill of materials (SBOM) and a hardware bill of materials (HBOM). This is a good starting point, though room for improvement remains. Once an organization receives an SBOM or HBOM from a supplier, they then need to analyze a (generally) manually crafted and error-prone set of data for supply chain threats. Hardware supply chains are straightforward, because you can generate a physical inventory and understand where components come from. When it comes to software, it becomes more difficult because we don't have SBOMs flowing through supply chains that are accurate and readily available. Some vendors are aware of the deficiencies and gaps in this process, but in our experience, many are not. Even those that are must rely on trust of sub-tier suppliers to ensure that proper security measures are being implemented.

Scaling and implementing this approach within the private sector presents unique challenges and should be evaluated as a possible solution only as part of a broader coalition of industry participants to ensure all potential barriers have been considered.

Regarding source code analysis, this is generally not very effective because that code could change or not even be present in the final firmware image that the device runs. It is critical that the final firmware image is what is analyzed[3].

[3] The UK Huawei Cyber Security Evaluation Center best demonstrated this problem by analyzing Huawei source code but failing to achieve "binary equivalence." Thus, the findings were effectively nullified. In contrast, Finite State analyzed final firmware images of Huawei devices and found numerous supply chain security issues that could be directly tied to production devices. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

Ultimately, the best approach is to evolve away from a vendor trust-based model, which prioritizes lightweight assessment of vendor processes, to a more robust and comprehensive approach, where every device and software application being placed within the BPS networks is being screened continuously for real threats and vulnerabilities. We are of the belief you need to have a trustless system and must be able to verify security and integrity based on the final firmware image. We need to have a verification system in place to generate an SBOM including snippets of code buried in binaries where backdoors can exist. All of that software must be tied to the vendors that built it, then tied to the country of origin.

This will take time and resources, including solutions similar to the capabilities our team and others offer and that continue to evolve as well, but may be a starting point for consideration as part of planning to move supply chain security forward within this industry.

c. assets and services critical risk tolerance regarding protecting these assets and services from FOCI?

Most organizations in the electric energy sector have defined processes for assessing and identifying critical assets and critical cyber assets, which was the initial approach in implementing North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements. These processes are often leveraged to inventory and prioritize assets and components for supply chain risk assessment. Even organizations that do not meet the medium and high thresholds have typically completed some analysis along these lines. Once an organization has an understanding of the risk for each asset, software, component etc., supply chain specific risk-assessments can be completed, including for FOCI risks.

The biggest challenge is that the industry is leveraging manual processes, typically on an entity-by-entity basis. Supply chain risk data is complex and nuanced and it is important to leverage tailored risk models to make it understandable and relatable to asset owners. Better standardized or large-scale solutions that allow entities access to data and tooling to help aid these decisions would be more effective.

(A-3) Are non-standard incentives or changes to established standard development organizations' SCRM standards (including NIST 800 series, ISA/IEC 62443, NERC-CIP, and other Cyber Risk Maturity Model evaluations/practices) necessary to build capacity to protect source code, establish a secure software and firmware development lifecycle, and maintain software integrity? How are benchmarks documented and tracked, including:

Standards are helpful, but they have to be developed with great flexibility, which may limit the extent of guidance that is available. Furthermore, they do not, in and of themselves, provide access to solutions or tools.

Non-standard incentives are an optimal solution. These should include consideration of the broad spectrum of organizations and their capabilities (e.g, size, type, scale, resources). Any approach should also consider risk -- not every entity poses a risk or the same risk to the BPS, and operational risk that does not present a security risk outside of that organization may not need to be considered. Additional input regarding the specific questions is provided below.

a. The ability to provide software, firmware, and hardware "bill of materials" (e.g. NTIA Software Component Transparency [see https://www.ntia.doc.gov/SoftwareTransparency] or equivalent industry norm) and track supply chain provenance and white-labeling;

First, generating a SBOM for any embedded device (including ICS/OT and IoT devices) remains with little standardized guidance. While it may seem as simple as producing a list of "ingredients" that are used in a product, it turns out to be much more complicated for embedded systems. Many software packages and platforms are provided to the Original Equipment Manufacturer (OEM) in binary form. Those binaries are difficult or impossible for most OEMs to analyze without advanced tools (such as the Finite State Platform). Even if software is provided in original source code form, there is still significant work required to understand exactly what open source and third-party components may have been included. An adequate solution likely requires a combination of manual efforts and investment in tooling.

Additionally, once a BOM is generated by a vendor, the downstream customers need to analyze that bill of materials. This is where lack of standards presents the biggest challenge. Each vendor has significant flexibility today in how they name each component and how deeply they look when identifying components (i.e. do they also identify statically linked libraries in binaries). The lack of a centralized database or standards for naming makes it very difficult for consumers of these bills of materials (BOMs) to use them for risk management (e.g. by comparing them to known threat and vulnerability databases). For example, when looking at a common software component, there could be upwards of 30 different names for it, making comparative and threat analysis extremely challenging.

As supply chain security evolves, vendors will need to be able to provide additional transparency to their customers via software, firmware, and hardware BOMs. Additional standards and investment are required to make this possible and to ensure information is accurate, consumable, and available. Having this type of information would provide the industry much better access and leverage to more efficiently evaluate supply chain risks.

Having standards to ensure compatibility and support funding for labor and tools would go a very long way, but there is still more work to be done. Accurately understanding comprehensive supply chain provenance and white-labeling requires tools that can accurately analyze the final, binary form of software and firmware and understand their provenance. While vendors like Finite State have invested substantially in building and implementing the capabilities to automatically conduct that type of assessment, this field continues to evolve and will be greatly enhanced by both vendor standards and increased participation within the energy industry.

b. authentication practices that prevent tampering, unauthorized production, and counterfeits; and

There are a number of anti-tamper approaches for electrical and mechanical systems which have proven effective. We are not addressing those in detail here but will note that from a firmware standpoint, each firmware image can be directly correlated to a unique hash and if any firmware image has been tampered with, that hash will change. In order to leverage hashes effectively as an anti-tamper approach, an entity must have secure means to transfer or host firmware updates, and then must check the hash before provisioning the firmware to ensure that it hasn't been tampered with.

c. monitoring and tracking sub-tier supplier's adherence to security requirements as part of the SCRM?

The sub-tier supplier risk problem is a well known and relatively unsolved problem in the industry due to the exploding number of suppliers involved in modern product development. The first step in monitoring and tracking your sub-tier suppliers is to know who your sub-tier suppliers actually are. Right now, neither asset owners nor OEMs have a comprehensive understanding of their sub-tier suppliers due to the lack of consistent, standardized bills of materials and supplier identification data throughout the supply chain.

Due to the challenges associated with merely identifying sub-tier suppliers, few if any asset owners or OEMs monitor or track sub-tier suppliers' security processes. Even if sub-tier suppliers are identified, they are subject to security reporting requirements from their direct customers, and thus, without standardized security reporting at each link in the supply chain, the quality and type of security data received is highly variable and difficult to interpret.

The explosion of sub-tier suppliers and the consideration of non-standard suppliers such as open source software providers is the primary reason that a shift from a vendor trust- and process-based approach to a vulnerability and threat verification approach is recommended. All of the data required to make an assessment of the product is available in the hardware, software, and firmware of the device and can be clarified by receiving BOMs from the OEM. Tools such as the Finite State Platform can make sense of this data

and provide accurate assessments of product, software, and firmware risks in a more concrete manner than vendor assessments would provide.

While non-standard incentives might alleviate some of the challenges associated with tracking sub-tier suppliers, we feel that verification of firmware components and their sources would render those incentives unnecessary, as the data would be able to provide the necessary information without having to track processes.

(A-4) What information is available concerning the following: BPS electric equipment cyber vulnerability testing standards, analyses of vulnerabilities, and information on compromises of BPS electric equipment over the last five years, including results of independent BPS electric equipment testing and penetration testing of enterprise systems for vulnerabilities (including methodology for discovery and remediation)?

> **a. What process does the energy sector have to share information with utilities regarding vulnerabilities and vice versa? Are contingency plans in place? How is the effectiveness of vulnerability testing and mitigation efforts monitored, tracked, and audited?**

There are several different standards for vulnerability and penetration testing of critical equipment being deployed by asset owners. For example, there are the NESCOR[4] standards which document a robust process for conducting vulnerability testing and reverse engineering to assess the attack surface, vulnerabilities, supply chain risks, and overall resilience to attack for a given piece of equipment.

There are limitations, however, on the ability to maximize usefulness of these. For example, entities that run these tests are typically prohibited from sharing results with other entities due to the contracts established by the penetration testing companies. The companies will generally resell the same test to multiple entities to increase their profitability. These manual penetration tests and vulnerability scans typically result in a report that represents a *single point in time exercise*. If a new version of firmware or software is released, the entire exercise would have to be repeated, which is not always the practice and would be costly and impractical. Additionally, as new vulnerabilities (such as the recent RIPPLE20) or supply chain threats are identified, there is no data generated during this process that allows for easy, retroactive analysis.

A collaborative, mostly automated, scalable approach for analyzing the BPS equipment firmware and software either in real-time or more frequently would solve most of these challenges and significantly increase security. Finite State has demonstrated the feasibility of this approach in several places throughout the supply chain so we are certain this capability and outcome are possible.

[4] National Electric Sector Cybersecurity Organization Resource

b. Is a record of an analysis of component vulnerabilities and any compromises of components and systems maintained for a specific period of time (e.g., five years)? If yes, are the results of independent component testing and penetration testing of enterprise systems for vulnerabilities (including timeline for discovery and remediation) also maintained?

Pen testing is a single point in time exercise. Standard practice is that pen test results can't be shared, therefore there is a massive amount of duplication. As noted above in the above responses, scalable vulnerability assessment capability is needed for firmware and devices.

d. How are vulnerabilities identified by external entities addressed? How is the distribution of information regarding patching security vulnerabilities in the supply chain facilitated?

Verification and standardized processes to track and share vulnerabilities are important and necessary to the overall security of any system. Verification must include deep firmware analysis to reveal the software components within BES and other critical infrastructure, and there must be a method to quickly and broadly distribute such information. Currently there are some information sharing centers and groups leveraged by industry, but they are typically restricted to select security professionals and participating organizations. This furthers an important security objective, but is counter to the ability to obtain input and data points from others that may be critical to preventing larger scale risks, assessing and applying lessons-learned, Evaluating the current information sharing structures and identifying better solutions that drive more broadly disseminated and discussed vulnerabilities and collaborative efforts for solutions would support the DOE objectives to improve supply chain security for BPS.

(A-6) Can energy sector asset owners and/or vendors document the level of engagement in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise (e.g., Information Sharing and Analysis Center, Information Sharing and Analysis Organization)? Does the energy sector participate in a community for sharing supply chain risks? Does the energy sector encourage security related information exchange with external entities, including the Federal government?

Sharing and leveraging the community at large is important. Incentives would be good to drive this, but there are scalable solutions that exist.[5] Information sharing with regards to supply chain threats is currently limited by the lack of streamlined processes and scalable solutions being utilized by energy sector asset owners and device manufacturers.

[5] Finite State, our organization, has built a system that not only analyzes firmware at scale, but encourages and allows those results to be shared between asset owners and device manufacturers to create a feedback loop to encourage better informed remediation.

Penetration tests, in addition to being point in time exercises, are not scalable, not standardized, and their results are not shared among entities and thus the usefulness of these efforts to broader security goals are limited.

B. Economic Analysis
As this RFI covers the full scope of BPS electric equipment as defined in E.O. 13920, the Department seeks information responsive to the following questions:

(B-3) Does the energy sector have a procedure to identify services, components, and/or systems which are or should be covered by E.O. 13920? If yes, list the services components, and systems and provide the reasoning regarding why they should or should not be covered by E.O. 13920.

Identifying such services, components, or systems would require a significant effort because doing so is difficult without analyzing device firmware, which may require a combination of tools and manual processes.

(B-4) What unique challenges could E.O. 13920 present to small businesses?

One of the primary challenges for small businesses is the lack of funding and insufficient team resources to address the myriad of issues and emerging threats. Many smaller companies do not have dedicated expansive security teams and resources ready to be able to tackle new threats, procure and deploy newer technology or tools and manage additional workloads as these threats expand.

The best solution would be an automated and scalable solution. It would allow smaller and resource constrained organizations to quickly and easily find and address vulnerabilities. Additionally, collaborative information sharing capabilities would prevent small businesses from having to expend additional resources to uncover vulnerabilities that have already been addressed by other or larger companies.