Strengthen the Resilience of America’s Critical Infrastructure

Cisco Response to the United States Department of Energy (DOE) Ensuring the Continued Security of the United States Critical Electric Infrastructure Request for Information (RFI)

Document No. 2021-08482
June 7, 2021

Cisco Response to RFI

Cisco Response to the U.S. Department of Energy Ensuring the Continued Security of the U.S. Critical Electric Infrastructure

Document No. 2021-08482

June 7, 2021

Cisco Systems, Inc.
http://www.cisco.com

June 7, 2021

Via Electronic Submission
ElectricSystemEO@hq.doe.gov

Cisco Systems, Inc. is pleased to submit the attached response to the U.S. Department of Energy Request for Information (RFI) for Ensuring the Continued Security of U.S. Critical Electric Infrastructure.

Technical and administrative questions regarding this response should be sent to Mr. Cannon Duke. Contact information is provided below.

Mr. Cannon Duke
Account Manager
Federal Scientific Region
Cisco Systems, Inc.
202-220-2425 (Office)
cannduke@cisco.com

Thank you for considering Cisco products and services for this opportunity. We look forward to working with the Department of Energy in support of this effort.

Sincerely,

Cannon Duke
Account Manager, Federal Scientific Region
Cisco Systems, Inc.

Table of Contents

List of Figures

Executive Summary

Cisco Systems, Inc. is pleased to respond to the Department of Energy's (Department) Request for Information (RFI) on Ensuring the Continued Security of the U.S. Critical Electric Infrastructure and provide our perspectives and insights as it relates to helping ensure critical electric infrastructure security.

The RFI and the Executive Order that precipitated it reflect a concern by the U.S. government about the necessity of managing risk from Actions to limit the adverse impact of foreign adversary ownership, and control of companies that produce key components used in critical electric infrastructure used in the United States, as discussed in this RFI, are certainly important considerations. In addition to managing for such risks, there are overarching concerns about the vulnerability of networked electricity grids to cyberattacks that require additional focus. Recent recommendations include requirements to acquire critical infrastructure components only from Original Equipment or Component Manufacturers or their authorized resellers, whenever available.

In addition, Cisco believes that there are now technical means and capabilities that should become part of a longer-term strategy for protection of U.S. critical infrastructure. The arrival of artificial intelligence and machine-learning-driven technologies over the past several years have not only increased the threat to our informational and operational technologies and systems, they have also dramatically improved the ability to protect associated critical infrastructures. These Trustworthy technologies, including capabilities to digitally sign the software image; securely boot hardware; establish a chain of trust for critical software; and use trust anchor chip modules as well as run-time defenses, can help enable electric utilities to more effectively secure their critical infrastructures.

There have also been recent initiatives by the Federal Energy Regulatory Commission (FERC) that move toward enhancing security by incentivizing electric utilities to voluntarily improve their security postures by implementing capabilities that provide automated and continuous monitoring; access control; data protection; and incident response, aligned with the National Institute of Standards and Technologies' (NIST) Cybersecurity Framework. We believe any additional security measures proposed by the Department should be aligned with the NIST framework and Reliability Standards developed by the North American Electric Reliability Corporation (NERC). To the extent that there are gaps identified in those approaches, they should be addressed through further industry-led standards development, to which regulatory requirements can then be mapped. Any other approach risks misaligning efforts to manage shared risks in an interconnected electric system that runs across shared borders with Canada and Mexico.

The above technologies and initiatives could become key foundational elements in a long-term strategy to provide more effective security to our nation's critical electric infrastructure. Cisco is pleased to provide more detailed comments in response to your RFI questions, as well as additional strategic inputs to inform your long-term strategy development.

A. Development of a Long-Term Strategy

A long-term strategy by the Department of Energy to protect our nation’s critical electric infrastructure should require not only non-adversary sourced infrastructure, but also that any infrastructure that is used in our critical electrical infrastructure be protected with advanced technical means to improve the trustworthiness of those systems.

Foundational to the long-term success of such a strategy is to begin incorporating existing protective technologies into our critical electric infrastructures. Specific examples of existing capabilities that could be harnessed through procurement requirements to better protect our critical electric infrastructure include:

- **Digitally sign the software image:** A two-step process for creating a unique digital signature for a given block of code. First, a hashing algorithm, similar to a checksum, is used to compute a hash value of the block of code. The hash is then encrypted with a private key, resulting in a digital signature that is attached to and delivered with the image. Signed images may be checked at runtime to verify that the software has not been modified.
- **Secure boot:** Helps to ensure that the code that executes on hardware platforms is authentic and unmodified. Hardware-anchored secure booting protects the micro loader (the first piece of code that boots) in tamper-resistant hardware, establishing a root of trust that helps prevent devices from executing tainted software.
- **Chain of trust:** The integrity of each element of code on a system is validated before that code can run. A chain of trust starts with a root of trust element. The root of trust validates the next element in the chain (usually firmware) before it can start, and so on. Using signing and trusted elements, a chain of trust can be created, which boots the system securely and validates the integrity of software.
- **Trust Anchor module:** Use of a tamper-resistant chip that features nonvolatile secure storage, Secure Unique Device Identifier, and crypto services, including random number generation (RNG), secure storage, key management, and crypto services to the running OS and applications.
- **Runtime defenses:** Target injection attacks of malicious code into running software. These runtime defenses can include Address Space Layout Randomization and Built-in Object Size Checking, to name a few.

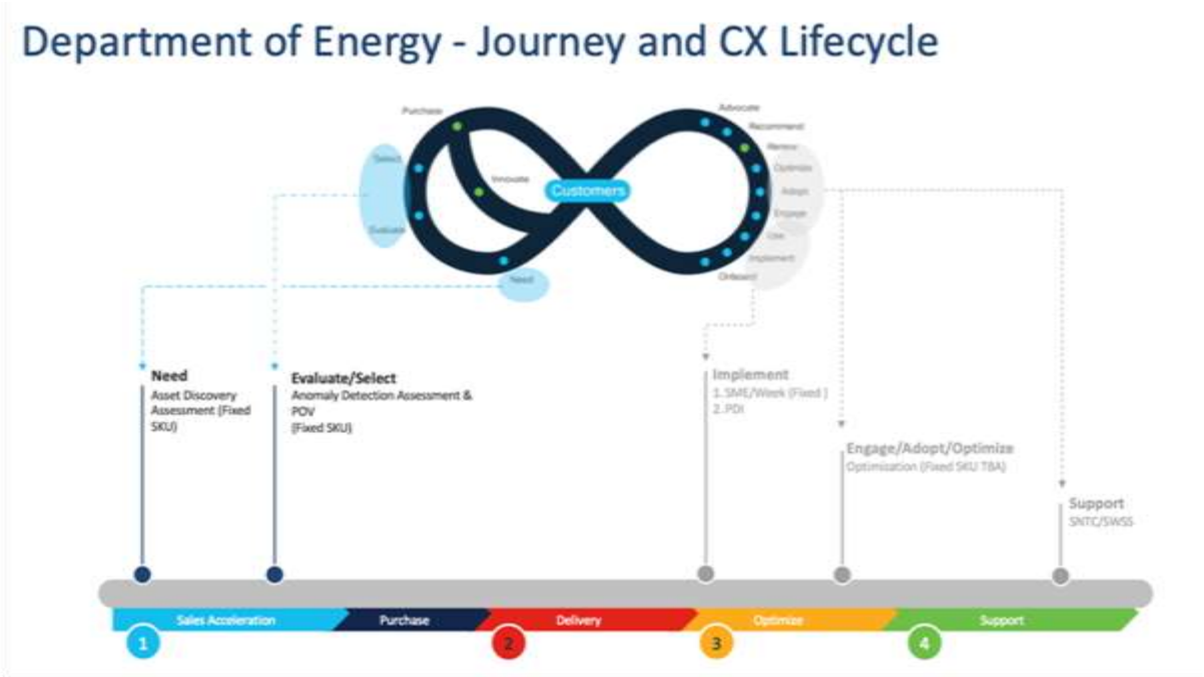
NIST has been working with industry over the last several years to leverage technologies with these types of protections. Support for using constructs like trust anchors was identified by NIST as long ago as 2015 in their Special Publication 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*. In addition, there is currently a project underway at NIST’s National Cybersecurity Center of Excellence (NCCoE) focused on the use of standards, best practices, and commercially available technologies to protect the digital communication, data, and control of cyber-physical grid-edge devices within our energy systems. See NIST Special Publication 1800-32, *Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources*, for details of this effort. Cisco responses to your specific RFI questions follow.

1. ***What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?***

Three key areas of technical assistance that would benefit States, Indian Tribes, and local governments relate to training, adoption of lifecycle approaches, and use of reference architectures related to protecting our critical electric infrastructures. The following examples (with a link to the Networking Academy Website and figures) are a piece of the Cisco ongoing Secure Grid development that will offer continuous development for security design, support, and ongoing education for employees.

Current offering examples include:

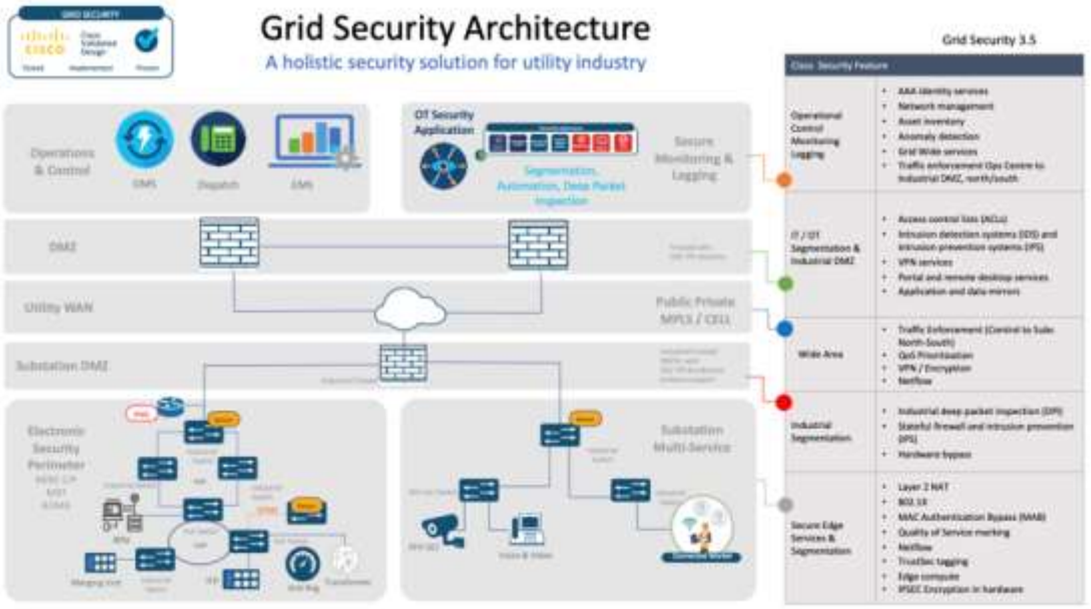
- Cisco Networking Academy for Training, Certifications, and Continuing Education. Refer to Cisco Networking Academy at https://www.netacad.com/.
- Lifecycle journey for full implementation, optimization, and ongoing critical infrastructure support (see **Figure 1**).
- Cisco Validated Designs and Reference Architectures for Electric Grid Security (see **Figure 2**).



Department of Energy - Journey and CX Lifecycle

6085p001

Figure 1. Customer Experience Lifecycle Technical Help and Implementation


Grid Security Architecture
A holistic security solution for utility industry
Grid Security 3.5
Operations & Control
DMS
Dispatch
EMS
OT Security Application
Segmentation, Automation, Deep Packet Inspection
Secure Monitoring & Logging
DMZ
Utility WAN
Public Private MPLS / CELL
Substation DMZ
Electronic Security Perimeter
Substation Multi-Service
6085p002

Cisco Security Feature	
Operational Control Monitoring Logging	AAA Identity services Network management Asset inventory Anomaly detection Grid Wide services Traffic enforcement Ops Centre to Industrial DMZ, north/south
IT / OT Segmentation & Industrial DMZ	Access control lists (ACLs) Intrusion detection systems (IDS) and intrusion prevention systems (IPS) VPN services Portal and remote desktop services Application and data mirrors
Wide Area	Traffic Enforcement (Control to Subs North-South) QoS Prioritization VPN / Encryption Netflow
Industrial Segmentation	Industrial deep packet inspection (DPI) Stateful firewall and intrusion prevention (IPS) Hardware bypass
Secure Edge Services & Segmentation	Layer 2 NAT 802.1X MAC Authentication Bypass (MAB) Quality of Service marking Netflow TrustSec tagging Edge compute IPSEC Encryption in hardware

Figure 2. Cisco Validated Design: Electric Grid Security Architecture

2. ***What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?***

It is Cisco's view that supply chain risk management needs more focus on the holistic security of the lifecycle of key products and on the technical controls and integrity verification, rather than overly focusing on country of origin to decrease security risk. Devices destined for critical infrastructure should be evaluated for the security of the entire Value Chain of the product from design, to build, to delivery and operations, through end of life.

A secure Value Chain starts with a Secure Software Development Lifecycle, a repeatable and trackable process designed to increase product resiliency and trustworthiness. Next, a secure Value Chain involves secure and audited manufacturing and logistics where security findings are tracked and evaluated for risk of compromise. Furthermore, devices need trust anchor technologies to independently validate hardware and software to prove integrity. Additionally, the vendor should provide onboarding and operational processes to validate authenticity and prove integrity of the device.

3. ***What actions can the Department take to facilitate responsible and effective procurement practices by the private sector? What are the potential costs and benefits of those actions?***

The Department can facilitate more responsible and effective procurement practices by requiring the private sector to:

- Buy from authorized resellers of a vendor's product. Vendors should provide a list of authorized resellers and continually evaluate those resellers' procurement standards.
- Validate device integrity before on-boarding into their business or operational environments by requiring vendors to provide an integrity validation process as part of their procurement requirements.

These actions will not only increase the security of our critical electric infrastructures but will also increase automation and reduce operational costs. OEMs can provide acquisition financing assistance to reduce required capital expenses, enabling these benefits derived from modernized technologies to be achieved much more quickly.

4. ***Are there particular criteria the Department could issue to inform utility procurement policies, state requirements, or FERC mandatory reliability standards to mitigate foreign ownership, control, and influence risks?***

Cisco recommends that the following criteria be issued as requirements to guide utility procurement policies, regardless of where the technology is developed and by whom:

- Ensure procurement policies require identification and validation that devices are procured only from authorized resellers of a vendor's product
- Ensure vendors use a Secure Software Development Lifecycle that includes:
    - Hardened and secured software build environment
    - Secure coding standards and safe coding libraries
    - Testing for protocol robustness, vulnerabilities, and application security
    - A vulnerability policy and plans for handling security alerts.
- Only procure from vendors that employ Trust Anchor technology in a way that hardware and software verify authenticity
- Require vendors to provide an integrity validation process before onboarding a device into customers' networks
- Ensure vendor's supply chain networks have global resiliency to mitigate risk of disruption from single region sourcing.

B. Prohibition Authority

1. To ensure the national security, should the Secretary seek to issue a Prohibition Order or other action that applies to equipment installed on parts of the electric distribution system, i.e., distribution equipment and facilities?

Cisco understands that the current Administration shares significant concerns with its predecessor about the security of the electric power system—and this is prudent in light of recent ransomware attacks targeting critical infrastructure systems.[1] However, the approach represented in Executive Order 13920 introduces significant risk of confusion, which we believe should be resolved before new requirements are put in place for systems below 100,000 volts (100 kV).[2] In addition, we strongly urge the Department to align any extension of cybersecurity risk management requirements with the Reliability Standards developed by the North American Electric Reliability Corporation (NERC)—particularly if the intention is to address local distribution systems in the range of 69kV to 100kV.

Specifically, the temporarily suspended and now reinstated Executive Order and the since-revoked Prohibition Order included language that could misalign cyber risk management for the U.S. grid with the leading standard for securing Bulk Electric Systems (BES) developed by NERC at the Direction of U.S. Federal Energy Regulatory Commission (FERC).[3] Furthermore, language in the Department's RFI appears to compound the confusion by potentially seeking to impose additional security requirements on electric **distribution** systems—despite the fact that the Executive Order that is the genesis of the Department's efforts specifically rules out coverage for local distribution systems. Cisco believes that the way forward is to establish a clear record establishing a common understanding of the risks to be managed; the adequacy of current cybersecurity standards at managing those risks; the gaps that require additional attention; and additional efforts necessary to close those gaps in a manner best calculated to ensure alignment across the transnational grid we share with our neighbors across our northern and southern borders.

As the Department is aware, NERC is dedicated to managing and mitigating security risks to the electric grid shared by the United States, Canada, and part of Mexico.[4] Given the interconnected nature of this network and the dynamic nature of the risks shared across our borders, the Department should seek an approach for managing cybersecurity risks that threaten the electric grid that is adopted in all three countries. To that end, we recommend that the Department establish a record spelling out the specific areas of risk that it believes are not adequately addressed by the prevailing

[1] https://www.engadget.com/pipeline-ransomware-010631984.html

[2] https://www.nerc.com/pa/Stand/Pages/CIP0131RI.aspx

[3] NERC was directed to develop the CIP-013-01 Reliability Standard to address cybersecurity risk in Bulk Electric Systems by order of Federal Energy Regulatory Commission (FERC). https://www.ferc.gov/sites/default/files/2020-04/E-8_1.pdf

[4] The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. https://www.nerc.com/AboutNERC/Pages/default.aspx

NERC standard CIP-013-01, and then work towards closing those gaps that are identified as requiring additional attention.

The FERC Order and the resulting NERC Reliability Standard aimed at addressing cyber risks in electric systems references a specific term, "Bulk Electric Systems" (BES). However, the Executive Order introduces a new term, "Bulk-Power System" (BPS), which appears to have somewhat different coverage. According to the Executive Order:

> *(a) The term "bulk-power system" means (i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more but does not include facilities used in local distribution of electric energy.*[5]

It is our understanding that the NERC CIP-013-01 Reliability Standard is focused on managing risks in electric transmission systems above 100kV. If the Department or the Administration has information indicating that there is a gap in current cybersecurity risk management practices that requires addressing systems in the range of 69kV to 100kV, we believe it is necessary to share that information with the owners and operators of such systems. Once a record has been established with public comment, it may then follow that FERC should direct NERC to reevaluate the current standard with an eye towards extending its coverage to additional systems or developing an additional Reliability Standard specific to such systems—e.g., transmission or distribution systems between 69kV and 100kV.

In the absence of such steps, industry faces significant confusion stemming from the use in the Executive Order of terminology (BPS) that does not readily map to the terminology found in the prevailing NERC Reliability Standard (BES). As noted above, the RFI appears to propose extending coverage of any new cybersecurity requirements it seeks to promulgate to distribution facilities—even though the Executive Order directing the Department to undertake this line of effort explicitly scopes out local distribution facilities from its coverage.

Specifically, the Department's RFI states:

> *Due to the interconnected nature of the U.S. transmission and distribution networks across the U.S., the Department is requesting comment on the advisability and feasibility of an expanded approach that would cover distribution facilities that serve CDFs.*[6]

By contrast, as noted above, the Executive Order states that its newly defined term "BPS" **"does not include facilities used in the local distribution of electric energy."**

In raising this point, Cisco is not controverting the notion that electric systems between 69kV and 100kV—including potentially distribution systems—may require additional cybersecurity. However, Cisco strongly believes that the goal of achieving improved security for our nation's bulk-power

[5] Executive Order 13920, May 4, 2020 (emphasis added). https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

[6] https://www.energy.gov/sites/default/files/2021-04/RFI%20Ensuring%20the%20Continued%20Security%20of%20US%20Critical%20Electric%20Infrastructure%2004202021.pdf

systems is best achieved by clearly aligning the scope, requirements, and effective date of any future Department rulemaking under the EO to robust industry-led standards, including NERC CIP-013-01. To the extent that there are additional risks not captured by those standards in systems operating below 100kV, they should be carefully studied with an eye towards whether they, too, require inclusion in either future standards setting or rulemaking procedures.

2. ***In addition to DCEI, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure serving other critical infrastructure sectors including communications, emergency services, healthcare and public health, information technology, and transportation systems?***

As discussed above, Cisco believes that a Prohibition Order alone is insufficient to address the security issues of the supply chain in critical infrastructure. Technical controls and integrity verification are essential to ensuring that critical infrastructure remains operationally available in the United States.

3. ***In addition to critical infrastructure, should the Secretary seek to issue a Prohibition Order or other action that covers electric infrastructure enabling the national critical functions?***

Again, the Prohibition Orders alone will not have the biggest impacts on securing our national critical infrastructures. The following are some of the things that Cisco recommends to better protect the national critical electric infrastructure:

- Make conscious decisions about whether and how critical systems should be tied to the networks—particularly those with Internet connectivity. Operators and suppliers may seek to connect even critical systems purely as a matter of convenience, and this is the source of the most visible recent attacks. Intermittent connectivity is a compromise; however, disconnecting from the Internet may be the most effective way to secure truly critical systems.
- Limit the connectivity of the IT Systems to the Operational Technologies (OT) of Critical Infrastructures.
- Maximize the use of IT and OT Security architectures and supporting security and networking tools.
- Understand the design of the network, the number of hosts on the network, and create a "Gold Copy" baseline to allow all OT networks and systems to be repaired and restored.
- Once connections and dependencies are understood, then risks can be effectively modeled and managed using the power for visibility and control made possible by intelligently designed intuitive networks.

The industry has broadly accepted these recommendations, which are well documented in the NSA Cybersecurity advisory, found here: https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF.

4. ***Are utilities sufficiently able to identify critical infrastructure within their service territory that would enable compliance with such requirements?***

The current North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) guidelines do an effective job identifying critical infrastructure, facilities, functional entities, as well as ownership and participation of responsible parties. This framework seems to be well understood across the utility industry and should continue to be leveraged as the Department addresses enhanced security of the electric infrastructure.

In addition, 'critical infrastructure' has historically been associated with the Bulk Electric System (BES). The Department should consider extending cyber-security requirements (as well as cost recovery mechanisms) beyond the BES and into the distribution grid. As noted in NIST NCCoE efforts (e.g., Special Publication 1800-32A, etc.), the distribution grid is evolving to include more and more renewables, and it is therefore increasingly imperative that the distribution environment be protected from cyber-attacks or from becoming an entry-point for cyber-attacks into our critical electric infrastructures.

Legal Disclaimer

Thank you for the opportunity to submit this non-binding RFI response for your consideration. Please note that this RFI response may include proprietary, confidential, and/or trade secret information which, if included, will be clearly marked as such in the proposal. Any information that Cisco considers to be a trade secret will not be subject to disclosure under any public records act.

We may have referenced information about future technology such as products and features under development that are not generally available from Cisco today. Because this technology is in various stages of development, all information concerning this future technology, including whether we will continue development, its availability, pricing, and included features, is subject to change and will be offered on a when- and if-available basis.

Trademarks

Every effort has been made to identify trademark information in the accompanying text. However, this information may unintentionally have been omitted in referencing particular products. Product names that are not so noted may also be trademarks of their respective manufacturers.

Cisco is a registered trademark of Cisco Systems, Inc.

The Cisco logo is a registered trademark of Cisco Systems, Inc.