UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Notice of Request for Information (RFI) on	)	6450-01-P
Ensuring the Continued Security of the	)	
United States Critical Electric Infrastructure	)	

JOINT COMMENTS OF SOUTHERN CALIFORNIA EDISON COMPANY & PACIFIC GAS & ELECTRIC COMPANY

Southern California Edison Company ("Edison" or "SCE") and Pacific Gas & Electric Company ("PG&E," and "Joint Parties," collectively) respectfully submit these comments in response to the Request for Information ("RFI") issued by the United States Department of Energy ("the Department" or "DOE") on April 22, 2021.[1] SCE, an Edison International Company, is one of the nation's largest electric utilities and is headquartered in Rosemead, California. Edison serves nearly 15 million residents via 5 million customer accounts in its service territory across 50,000 square miles in Central, Coastal, and Southern California. Edison operates 118,000 miles of distribution and transmission lines and has committed to significant investment over the coming years to expand and strengthen its electric system infrastructure.

Edison and its holding company, Edison International, have long been recognized as leaders in the cybersecurity space and has a demonstrated history of executive-level participation in public-private partnerships to enhance the cybersecurity and resilience of the North American electric grid, including through its participation in the Electricity Subsector Coordinating Council (ESCC) and the Energy Cybersecurity Alliance, and dozens of other forums and initiatives.

A subsidiary of PG&E Corporation, PG&E is one of the largest combined natural gas and electric energy companies in the United States. Based in San Francisco, California, PG&E delivers some of the nation's cleanest energy to nearly 16 million people in Northern and Central California. Servicing approximately 5.1 million electrical distribution accounts and 4.4 million natural gas

[1] 86 FR 21,309.

distribution accounts, PG&E similarly seeks to uphold critical infrastructure security through its participation in multiple forums addressing security-related matters, such as the Edison Electric Institute ("EEI") and more.

Through its recent RFI, the Department has reiterated its commitment to ensuring the security of Critical Defense Facilities, a commitment which Edison and PG&E share. The comments included herein seek to propose actionable and targeted improvements on how the Department and its government partners can collaborate with Joint Parties and our peers to secure the supply chains of critical grid equipment against the risk of supply chain compromises. Such compromises seek to disrupt the security, safety, and well-being of Americans – including the millions who rely on Joint Parties to safely and reliably deliver electric power across California.

REGARDING DOE'S LONG-TERM SUPPLY CHAIN RISK MANAGEMENT ("SCRM") STRATEGY

In its RFI, the Department posed a number of questions regarding its long-term strategy to address supply chain risks, including the following:

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

II. *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?*

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

IV. *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?*

Joint Parties appreciate the Department's willingness to engage with the owners and operators of this critical electric infrastructure. We respectfully request that DOE and its government partners consider the following recommendations:

A. Drastically re-envision how supply chain threats are communicated to electric infrastructure owners and operators in a collaborative manner.

The need for improved information sharing has been highlighted in countless assessments in

recent years, notably including the July 2020 report from the Cyberspace Solarium Commission.[2] However, progress to-date has been insufficient. The private sector has dedicated significant investments in due diligence to investigate security risks to its electric infrastructure and assets. Yet, an absence of government-sourced threat intelligence regarding Foreign Ownership, Control, and Influence ("FOCI") persists. For example, the Administration named five countries of concern – China, Russia, North Korea, Iran, and Venezuela – but stopped short of providing the names of specific individuals, companies, and/or products that underlie the concern. More specific and meaningful disclosure would provide the actionable intelligence needed by the private sector to assist in addressing any gaps.

Joint Parties recognize that multiple policy and legal issues factor into the decision to name specific individuals or companies as being of concern. Joint Parties respect the difficulties facing the Federal government in making such determinations. However, this type of intelligence sharing is not without precedent; in response to national security concerns in communications and video teleconferencing equipment, the Department of Commerce added five covered suppliers to its Entity List. This provided the private sector with specific information that could be acted upon. Similar efforts to publicly provide this government intelligence on FOCI should be carried out to support protection of electric grid infrastructure.

Further, EEI's response to this RFI highlights the need for improved remote classified intelligence sharing. Joint Parties support EEI's response.

B. Clarify the specific equipment which the Department views as the highest risk, based on intelligence.

EEI's comments also highlight the utility sector's concerns that not all equipment faces the same degree of risk. For example, given their varied degrees of digitization and therefore their varied attack surface, solid state relays and microprocessor relays carry notably different cybersecurity risk profiles despite carrying out similar functions. In order to enable utilities to concentrate risk-reduction efforts that provide meaningful and demonstrable benefits, the Department and its government counterparts must provide clarity on which types of equipment represent the highest risk, based on the intelligence that they have assessed.

[2] Cyberspace Solarium Public Report | https://drive.google.com/file/d/1S5N7KvjFfxow19kCnPl0nx7Mah8pK0uG/view

Other utilities, including AEP, have further highlighted this need for clarity by urging the department to "state without ambiguity the level of component which is subject to them (e.g., chips, boards, subsystems, entire application, modules within an application, open-source components used within an application, operating system, firmware, etc.)." Without a targeted, clarified approach, valuable time and security resources will be spent making changes which introduce costs and complexity without sufficient justification, to the ultimate detriment of our customers.

Finally, should DOE implement this recommendation, Joint Parties note that access to such information will need to be tightly controlled, as such information would – if released publicly – enable malicious actors to tailor attacks against the grid. Such controls should apply to Freedom of Information Act requests, as well as released on "need to know" basis even to industry partners.

C. Evaluate market-based solutions to address the lack of domestic production for critical grid components.

Joint Parties agree with the Administration's stated policy to strengthen the resilience of America's supply chains, including the Energy Industrial Base.[3] The Department itself has previously recognized some of the supply chain constraints for critical grid equipment, including large power transformers. In recognizing the risk that is introduced through sourcing sensitive equipment from potentially adversarial nations, the Department must consider ways to help bridge the gaps where domestic sources for this equipment may not exist, or are otherwise insufficient or cost-prohibitive.

The Department should consider, among other solutions, market-based incentives to establish domestic manufacturing and production capabilities for sensitive grid equipment. This may include seed-funding to establish new domestic suppliers, or creating reliable cost recovery mechanisms to bridge the sometimes-significant gap between cheaper equipment sourced from potentially adversarial nations, and from domestic or friendly international suppliers. In

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

particular, where utilities make targeted security investments for the benefit of *national* security, DOE should consider cost recovery mechanisms that spread the costs of such investments across the nation as a whole*;* a utility's rate-base should not shoulder such costs where the actions are taken to protect national interests.

D. Expand supply chain equipment testing programs.

In order for the electric sector – and the nation – to meet ongoing security threats, it is imperative for this industry to identify vulnerabilities in the equipment comprising critical infrastructure. Expanded testing of critical OT equipment used by most utilities would help identify many of these embedded vulnerabilities, including backdoors, default credentials, out of date libraries or firmware, etc., and other potential attack vectors.

In order to address these threats, Joint Parties support programs such as the DOE's "Cybersecurity Testing for Resilient Industrial Control Systems" (CyTRICS) Program – an innovative program that enables equipment manufacturers to send their products to Idaho National Laboratory (INL) for advanced security and vulnerability testing. Thus, first, we encourage DOE to continue expanding CyTRICS, and other programs like it, such as the supply chain task force created by the National Defense Authorization Act of 2020 (NDAA 2020).

Next, the Department should consider incentives to encourage manufacturers to engage in this testing at the National Laboratories as well as through private-sector testing capabilities. We recognize that legislation may be required to fund such programs. This is an area that warrants a "whole of government" approach.

Finally, Joint Parties encourage equipment manufacturing industry leaders to participate in equipment testing programs through private arrangements with individual utilities. Joint Parties believe there is strong utility desire to partner with equipment manufacturers to perform joint vulnerability and security testing. However, such arrangements are still new, and thus face roadblocks related to liability, indemnification, and intellectual property (IP) protection concerns. These issues of national security require strong, concerted action between manufacturers of critical electric equipment, those who use this equipment, and the U.S.

government to overcome these roadblocks.

E. Take a forward-looking; risk-informed approach by working to design more secure devices.

Efforts to improve grid equipment supply chain cybersecurity must take a forward-looking, risk-informed approach to design more secure devices that ensure lasting improvements to grid security. Many utilities are making significant investments in their grids to improve reliability and resilience, and in support of their climate and clean-energy goals. For example, Edison reported around $5 billion in annual electric infrastructure investment opportunity in 2020[4] and estimates up to $75 billion in grid investments will be needed from 2030 to 2045 to integrate bulk renewable generation and storage and serve the load growth associated with transportation and building electrification.[5] In recognition of these significant investments and changes, the Department's long-term strategy should not only focus on the equipment used by utilities today; rather, they should be forward-looking to support lasting improvements over the coming decades.

To do this, DOE should expand upon its partnerships with utilities to enhance its understanding of grid modernization plans, with a focus on identifying future risks. This approach should be risk-informed, including consideration of affected customers, vulnerability of specific system components, built-in system redundancies, and ability of the utility to respond to an adverse outcome. Additionally, DOE should engage the developer and manufacturer communities to ensure the security of these devices from the earliest stages of product inception.

The Department should also firmly encourage state regulators and public utilities commissions to meaningfully support secure R&D activities to accomplish these goals. Under current regulations, utilities can be severely constrained in their abilities to engage in R&D projects. However, with improved incentives, which may include grants and allowable rate recovery for R&D activities, utilities can better collaborate with developers, manufacturers, research institutions, and the Department on forward-looking security projects.

[4] https://www.edison.com/content/dam/eix/documents/investors/sec-filings-financials/2020-financial-statistical-report.pdf
[5] https://download.newsroom.edison.com/create_memory_file/?f_id=5dc0be0b2cfac24b300fe4ca&content_verified=True

F. Issue consistent criteria and guidance for hardware and software bill of materials (HBOMs & SBOMs).

Hardware and software bill of materials are an additional tool to provide utilities with greater visibility into the devices and software that they are purchasing. This increased visibility in turn helps utilities identify potential concerns with an increased level of precision. However, the current lack of a standardized format for these HBOMs and SBOMs has made it difficult for suppliers to efficiently provide this information in a consistent or complete fashion. Recent government efforts, including the National Telecommunications and Information Administration ("NTIA") initiatives, to improve standardization in this area represent a valuable and important step, and Joint Parties encourage the Department to continue to support these efforts while prudently ensuring that this wave of new information does not offer adversaries another source of information which could be weaponized.

G. Expand efforts to improve security through the software lifecycle.

Joint Parties support the goals of the May 12 Executive Order on Improving the Nation's Cybersecurity[6], namely the improvements to the cybersecurity of software supply chains through improved management of open-source software, software bill of materials, incident reporting, and other measures. Joint Parties encourage the continued focus on this issue and collaboration with software developers and equipment manufacturers to further this work and expand these into the electric sector in a risk-informed fashion.

H. Increase support for small municipal utilities and electric cooperatives.

In recognition that supply chain compromises may impact utilities of all sizes and of all business types, including municipal utilities and electric cooperatives, the Department's long-term SCRM strategy should consider ways to support utilities of all sizes and business models. These often-smaller municipal utilities and electric cooperatives typically have fewer resources to establish comprehensive SCRM programs; as such, DOE should consider ways to help them address the specific challenges these utilities face. An example of this could include providing seed funding to establish improved third-party risk information sharing mechanisms. This would help socialize some of the costs associated with SCRM.

[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

REGARDING DOE's PROHIBITION AUTHORITIES

The Department expanded upon the long-term SCRM strategy questions and posed four additional questions to solicit feedback on its Prohibition Authorities.

I. *To ensure 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?*

II. *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?*

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

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

Joint Parties encourage DOE to consider the following factors in its review of future prohibition authorities:

A. Critical Defense Facilities represent a strategic focus and a shared industry-government priority.

Recognizing the important role these Critical Defense Facilities play in ensuring the continued ability for the United States Military to protect the homeland and our people, Joint Parties support the Department's primary focus on these facilities. As such, the protection of these facilities should remain the primary focus for the Department's Prohibition Authorities.

B. Significant work has been done to coordinate between interdependent critical infrastructure sectors.

Representatives from the electric, communications, and financial sectors have been engaged in ongoing collaborations for several years to improve coordination between these three essential sectors. And as recently as 2020, a cross-sector coalition consisting of leaders from the energy and financial sectors stood up a similar joint organization – the Analysis and Resilience Center

– aimed at protecting the nation's most critical infrastructure from systemic risks.[7]

EEI, in its comments, offers several other examples of meaningful industry-driven collaborations. Recognizing that significant progress has been made through these efforts, any blanket government actions in this space risk upending the progress of existing efforts, to the net detriment of collaboration and security. Further, there are no "one-size-fits-all" approaches that would benefit all sectors which would not also, by their very nature, impose significant and undue cost to customers. As such, future DOE engagements to address cross-sector interdependencies must be approached in a targeted, risk-informed fashion, with the highest-risk areas addressed first. Also, DOE engagements should first consider existing structures and processes, and, to the maximum extent possible, leverage these pathways before creating entirely new and possibly reductive regimes.

C. Coordination between DOE and State regulators would support the alignment of efforts across all levels of government.

Electric utilities today are subject to cyber and physical security regulation at a variety of levels, including by the Federal government at the transmission level, and by state public utilities commissions such as the California Public Utilities Commission ("CPUC") at the distribution level. As state regulators have decades of experience working with critical infrastructure owners and operators in their states, it is important that DOE coordinates with these state bodies to gather information on their existing authorities and other valuable insights. Groups such as the National Association of Regulatory Utility Commissioners ("NARUC") and National Association of State Energy Officials (NASEO) should also be consulted as they offer a national-level perspective on these state-based considerations.

Finally, Joint Parties encourage DOE to continue seeking industry input. For example, the California utilities were heavily involved in working collaboratively with CPUC in the development of CPUC's 2020 physical security regulations – a process that CPUC staff

[7] https://SystemicRisk.org

described as collaborative.[8] Similar utility involvement would aid DOE and state regulators develop strategies for protecting the distribution grid that reflect state/federal needs, along with operational realities.

D. Security and resilience are cross-functional and often intersectional; as such, cyber and physical security should be considered as complementary and approached holistically.

The Department's RFI focuses on meeting cybersecurity risks. However, Joint Parties respectfully urge DOE, and the Federal government in general, to continue addressing risks to energy security that exist outside of the digital arena. Physical threats such as armed human attack, explosive devices, and weaponized drones also must be addressed. An attacker seeking to disrupt electrical services may even employ hybrid attacks against a utility's cyber and physical defenses simultaneously.

E. Strengthen DOE's status as a proactive industry partner.

In protecting the nation's cybersecurity, DOE has been commendably proactive in developing collaborative cybersecurity programs with private industry partners. Programs such as CyTRICS, listed above, or the Cybersecurity Risk Information Sharing Program (CRISP), are two such examples. Regulated entities may also be encouraged to participate in such programs with DOE.

Industry, and Joint Parties in particular, values DOE's openness and flexibility in developing national security programs essential to our nation's survival. As the nation's posture towards cybersecurity and national security evolves, Joint Parties respectfully urge DOE to maintain its ability to continue developing these collaborative programs as the energy sector's Sector

---

[8] SED Staff Workshop Notes, for Workshop Dated May 2, 2017, at p3. The PFM Parties filed the workshop notes, with proposed edits, at the CPUC: Pacific Gas and Electric Company's (U 39-E), Southern California Edison Company's (U 338-E) and San Diego Gas and Electric Company's (U 902-E) Joint Comments and corrections to Combined Workshop Notes, Rulemaking 15-06-009 (July 28, 2017), at http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M195/K910/195910875.PDF (CPUC staff describing utilities' receptiveness to collaborate with CPUC); https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/Final

The foregoing filings were made in CPUC Rulemaking No. R.15-06-009, Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electrical Corporations Consistent with Public Utilities Code Section 364 and to Establish Standards for Disaster and Emergency Preparedness Plans for Electrical Corporations and Regulated Water Companies Pursuant to Public Utilities Code Section 768.6.

Specific Agency and Sector Risk Management Agency.

CONCLUSION

Joint Parties appreciate the opportunity to provide these comments for the Department's consideration and supports the Department's focus on addressing the very serious supply chain risks which are faced by the electric subsector. The security of Critical Defense Facilities in particular represents a mutual and strategic concern. Joint Parties are committed to working collaboratively with the Department to support these facilities and their important role in defending the Homeland and its people, including the millions of Americans across our respective service territories. We look forward to further thought collaboration and exchanges on these all-important areas in support of energy security and national security.

On Behalf of Southern California Edison Company
& Pacific Gas & Electric Company

Respectfully Submitted,

Kegan Gerard
Cybersecurity Advisor
Southern California Edison
2244 Walnut Grove Ave
Rosemead, CA, 91770
Email: Kegan.Gerard@sce.com