



TRANSMITTED ELECTRONICALLY THROUGH REGULATIONS.GOV

June 7, 2021

Mr. Michael Coe
Director, Energy Resilience Division
Office of Electricity
U.S. Department of Energy
Mailstop OE-20, Room 8G-042
1000 Independence Avenue SW
Washington, DC 20585

Subject: Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

Dear Mr. Coe,

UL appreciates the opportunity to comment on the Department of Energy's "Notice of Request for Information on Ensuring the Continued Security of the United States Critical Electric Infrastructure" to President Biden's January 20th Executive Order 13990, *Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis*. In August 2020, UL submitted comments to the Department on the previous Bulk Power System Executive Order and accompanying RFI and is eager to continue the dialogue with the Department on this important issue. UL applauds the efforts and actions that President Biden and the Department's already taken to secure the nation's bulk power systems (BPS) and to increase security of other critical infrastructure.

UL supports the Department of Energy seeking information to understand how to best exercise its role as the Sector Risk Management Agency, to respond to the threat landscape and how to best protect critical infrastructure. Specifically, UL applauds the Department for the consideration given to critical infrastructure facilities beyond the December 2020 prohibition order to include distribution facilities that serve critical defense facilities (CDFs) and other non-defense but otherwise critical national infrastructure such as communications, emergency services, healthcare/public health, information technology, and transportation systems.

Since its inception in 1894, UL serves a mission of promoting safe living and working environments for people everywhere and fulfills a promise of facilitating the flow of goods across borders. Grounded in science and collaboration, UL's work empowers trust in pioneering technologies, from electricity to the internet. We help innovators deliver safer, more secure products and technologies through a wide range of research, standards development, and testing and certification services.

In a connected world, safety cannot exist without cybersecurity. Building off our safety reputation, UL supports our customers and stakeholders with their grid cybersecurity needs, in part, by helping to foster collaboration up and down the supply chain. A byproduct of this collaboration is UL's scalable suite of cybersecurity solutions and certifications.

UL's Supplier Cyber Trust Level is one example of a comprehensive supply chain risk management solution covering security controls from many well-known industry best practices, standards and

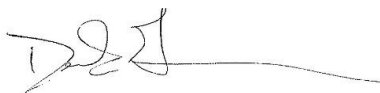
frameworks. UL's Supplier Cyber Trust Level assessment enables a holistic view of a supplier's security posture, while providing a fair and consistent evaluation for organizations of the cybersecurity posture from supplier to supplier. The UL Supplier Cyber Trust Level leverages security controls from many well-known industry best practices, standards and frameworks, including National Institute of Standards and Technology (NIST) cyber supply chain risk management, European Union Agency for Cybersecurity (ENISA) supply chain attacks, NERC CIP-013-1 regulation and standard, IEC 20243-1 standard, ISA/IEC 62443-4-1 and ISA/IEC 62443-2-4 standards and the ISO 27001 standard, among others.

UL is actively engaged in the industry and educating utility and supplier stakeholders regarding cybersecurity risks and solutions. This includes collaboration with the North American Transmission Forum (NATF) and mapping UL's Supplier Cyber Trust Level to NATF Cyber Security Supply Chain Criteria for Suppliers, among actively discussing with and advising other important industry stakeholders.

In addition, UL is supportive of and provides services to existing standards and solutions in adjacent industry verticals such as ISA/IEC 62443 standards and certification, gaining adoption in industrial automation including among electrical grid suppliers, next to standards for Enterprise Resource Planning (ERP) systems such as ISO 27001, NIST SP 800-53 or NIST SP 800-171. In the European Union, following the NIS Directive, emphasis has been placed on ISO 27001, and ISO 27019 as dedicated to utilities, for managing information and industrial control systems for cybersecurity. ISA/IEC 62443, and specifically the sub-standard ISA/IEC 62443-2-1, addresses both the asset owner or manager information management and control systems as the combined Cybersecurity Management System (CSMS) in scope, and the standard is likely to gain adoption also alongside ISO 27001 and ISO 27019 standards.

Please find below UL's responses to a subset of the questions posed in section II A of the Request for Information. As the Department of Energy moves forward with its efforts to secure the bulk power system and expand protections beyond strictly defense related infrastructure to other national critical infrastructure, UL is eager to share our valuable expertise with DOE. If you have any questions regarding this submission or would like to discuss UL's recommendations further, please do not hesitate to contact Thomas Daley, UL Global Government Affairs, at thomas.daley@ul.com. Thank you for your attention to these comments.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Derek Greenauer', followed by a horizontal line extending to the right.

Derek Greenauer
Americas Director, Global Government Affairs

A. Development of a Long-term Strategy

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?

UL supports a 'whitelisting' of suppliers supported by industry's independent assessment and review capability, employed to mitigate and manage supply chain risk short of issuing bans or blanket prohibitions that are based solely on origin. Determining provenance can be part of any supply chain risk management criteria, evaluation, and labeling program. As part of regulator-mandated or incentivized supplier assessments, and based on current industry best practices, suppliers provide bills of material for their digital, hardware and/or software (DBOM, HBOM and SBOM) which could be expanded to include the origin (such as countries where development environments and personnel are located) and movements (shipping logistics) of products, components and services, to establish product, component or service provenance. Suppliers can include this information for their suppliers or supply chains as well. As an example, UL is requesting this information as part of its Supplier Cyber Trust Level. An example of a standard or framework to base provenance criteria on, also included in UL's Supplier Cyber Trust Level, is IEC 20243-1 for integrity of hardware and software products through the product lifecycle to mitigate risks of tainted and counterfeit products. UL also advocates use of dedicated component security assessments, examples of which include long-standing FIPS 140-2/3 certifications for crypto modules, PSA Certified, an industry led certification program, or UL's Secure IoT Component Qualification. Combined, establishing provenance and validating implementation of security controls can help manage FOCI-related supply chain risk.

UL also asks the Department to recognize and align concurrent implementation of NERC-CIP-013-1 and ongoing efforts by utilities and suppliers to comply with the regulation.

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 should actively incentivize private sector procurement practices that prioritize supply chain risk management, especially when and where critical infrastructure is involved, such as emphasizing adoption of industry-standard based conformity assessment approaches, including those based on ISA/IEC 62443.

In order to prioritize supply chain risk management, there is a need to gain visibility about systems, products, components and services, as part of an IT and OT asset inventory. It is considered a necessity that operators of critical infrastructure have or will put in place an Asset Management System. The benefit is visibility, risk prioritization and faster response to any incident or vulnerability that becomes known.

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?

In addition to existing FERC mandatory reliability standards such as NERC-CIP-013-1, the Department should consider criteria that emphasize adoption of industry standard-based conformity assessment approaches. An example of a standard or framework to base criteria on is IEC 20243-1 for integrity of hardware and software products through the product lifecycle to mitigate risks of tainted and counterfeit products. More generally, other standards and frameworks help address cybersecurity risks such as ISO 27001 focused on the information security management system of the organization, ISO 22301 addressing business continuity management, ISA/IEC 62443-4-1 addressing the secure development processes for software and hardware components, products and systems, or ISA/IEC 62443-3 and ISA/IEC 62443-4-2 addressing security requirements for industrial automation and control systems and products, at the system- and product levels.