

**Native American Industrial Solutions LLC  
And  
Eclipsium, Inc.**

**Response to Request for Information on  
Ensuring the Continued Security of the  
United States Critical Electric Infrastructure**

**Submitted to:**

U.S. Department of Energy  
[ElectricSystemEO@hq.doe.gov](mailto:ElectricSystemEO@hq.doe.gov)  
(202) 586-2036

**Submitted by:**

NAIS LLC  
14323 Ocean Highway, Suite 4119  
Pawleys Island, SC 29585  
[admin@nais-llc.com](mailto:admin@nais-llc.com)  
(845) 702-8323



---

**Table of Contents:**

**Cover Letter .....ii**  
**Questions and Responses.....1**  
**Conclusion .....5**

---

June 7, 2021

Energy Resilience Division  
Office of Electricity  
Department of Energy  
Mailstop OE-20, Room 8H-033  
1000 Independence Avenue, SW  
Washington, DC 20585  
**ATTN: Michael Coe, Director**

Native American Industrial Solutions LLC (NAIS), on behalf of itself and Eclipsium, Inc., consider it a privilege to submit our joint response to the Request for Information on Ensuring the Continued Security of the United States Critical Electric Sector, Docket # DOE-HQ-2021-08482, for the U.S. Department of Energy.

Native American Industrial Solutions LLC (NAIS) is an American Indian owned 8(a) company and a Service-Disabled Veteran Owned Business (SDVSOB) focused on providing IT and cybersecurity services and solutions. NAIS has three major lines of operation: Risk Management & Cybersecurity, IT Infrastructure Solutions and Services, and Software Development. Our team has performed exceptionally well on large contracts supporting the Defense Health Agency (DHA), first through Software Maintenance and Data Management and currently through Enterprise Systems Branch (ESB) services, providing support across Tiers 1 through 3 while providing Systems Administration and Cybersecurity & Information Assurance services. We also have ongoing contracts supporting the Department of Homeland Security (DHS) providing risk modeling, vulnerability management, and analytics, as well as supporting the Hunt & Incident Response Team (HIRT) program.

Through our tribally owned 8(a) Joint Venture (JV), we can receive sole-source contracts up to a ceiling of \$100M for goods and services in the DoD (based on the 2019 NDAA) and up to \$25M for goods and services for other federal agency contracts. Moreover, awards to tribally owned 8(a) firms are not protestable. The IVA'AL/NAIS Technologies Joint Venture (JV) is comprised of IVA'AL Solutions LLC and Native American Industrial Solutions LLC (NAIS). We bring together the nimble, white glove services of a small business and the resources and contracting flexibility of a large enterprise.

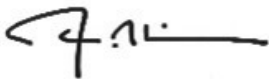
Eclipsium is a comprehensive cloud-based device security platform for modern distributed organizations. Eclipsium protects the devices that organizations rely on, all the way down to the firmware and hardware level. The Eclipsium platform provides security capabilities ranging from basic device health and patching at scale to protection from the most persistent and stealthiest threats.

The core members of NAIS and Eclipsium have a long history of service in the military and civilian government agencies. We are committed to bringing the highest levels of quality, service, and value to our customers. Individually and jointly, NAIS and Eclipsium possess the skills and capabilities necessary to assist the U.S. Department of Energy and the nation's bulk-power system in understanding and addressing supply chain risks and other vulnerabilities within the hardware and firmware upon which bulk-power system equipment depends.

With respect to our attached response, we maintain strong relationships with other vendors in this space and stand ready to provide a full package of solutions for evaluating, securing, and monitoring any IT, operational technology, or the supply chain environment.

If the opportunity presents itself to the Government and in accordance with the authority granted under FAR 6.302-5, authorized or required by statute, we would be pleased to explore opportunities to pilot some of the risk management approaches highlighted in our response with the U.S. Department of Energy, including the National Laboratories, and/or one or more utilities.

Respectfully,



Jeremy Meyers  
President & CEO  
Native American Industrial Solutions LLC

---

## QUESTIONS AND RESPONSES

E2 Hizipstq irx\$je\$Prk1Xivq \$wxexik}\$

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

State, local, tribal and territorial (SLTT) governments would benefit from technical assistance covering a few areas. First, due to the limited resources often available within SLTT governments, an assessment methodology that enables them to better understand their critical dependencies on the electric system would be helpful. Second, assistance in analyzing SLTT government supply chains would enable procurement decisions that are commensurate with dependency criticality levels. Third, if SLTT governments had access to trusted hardware, software, and firmware profiles such that they could compare those profiles to acquired assets, deviations from a trusted state could be measured and identified. This could be used during initial procurement, deployment, and operations and maintenance phases to make risk-informed decisions. There are a variety of federal government resources available. The Department of Energy might consider partnering with the Cybersecurity and Infrastructure Security Agency's regional forces, which can facilitate a Cyber Resilience Review assessment, which includes a component focused on external dependencies, as well as an External Dependency Management Assessment.

The need to identify trusted profiles at scale is driven by the current, common approach to supply chain security. Most supply chain security programs include contractual agreements and procedures but few technical details or assessment. The contractual language is often designed to establish parameters for risk transference, but generally focused on broad categories of activity and expectations, such as sourcing, the use of a defined development lifecycle, breach notifications, and others. If more technical detail were required, dedicated specialists would be required to perform analysis of various models of equipment and embedded components used. Instead, common tools for establishing and monitoring a baseline can be leveraged by the energy sector. Frameworks based on open source projects have been successful in lab environments and are generally considered limited in scope, but Eclipsium's commercial offering is currently available to bring a broader vendor independent and scalable approach into operational monitoring for an enterprise.

Eclipsium performs ongoing research into the security of firmware and hardware components used throughout enterprise systems. As part of this process, we coordinate with manufacturers, software/firmware developers, CERTs, and other organizations to ensure that updates become available to mitigate the issue. A timeline is generally contained as part of our public release on our research website (<https://eclipsium.com/research>). Our research into firmware and hardware vulnerabilities has provided first-hand experiences with multi-party vulnerability coordination related to components that are reused in the supply chain of many devices and systems. This work has driven us toward identifying technical mechanisms for detecting issues and building a profile for normal operation of devices and components. By realizing these mechanisms in an automated scanner and analytics platform, Eclipsium monitors key milestones in the supply chain, operations, decommissioning, and incident response.

While much of Eclipsium’s focus has been on monitoring, we suggest using our core capabilities around research and detection to develop trusted device profiles. First, there is a need to begin with a baseline profile for each device. This profile can be monitored across industry to see if changes are observed and whether those changes are benign and expected or undesired and unplanned. Primary inputs for analysis would be device and firmware configuration data and integrity checks. This can then be used to initiate deeper analysis of hardware, software, and firmware supply chains. Behavioral detection and machine learning-driven training models can be applied to continuously make sense of observations. To achieve sufficient observation scale, the Department could drive it through a NERC CIP update.

Depending on the Department’s interest, the scope of this approach towards identifying trusted profiles and monitoring for profile changes and associated threat activity could be scaled through a Department program that incorporates the Cybersecurity and Infrastructure Security Agency’s (CISA) industrial control systems operations. Specifically, the Department could leverage the cyber threat indicator sharing protections available to the private sector by directing electric system and vendor industry participants to contribute observations via already-existing CISA ingest channels. The Department and CISA could then collaboratively analyze cyber threat indicator observations alongside an increasingly large device profile dataset. While this information, under law, can not be used to take regulatory enforcement action, it could be used in the aggregate to inform future regulations. Operationally, however, it could be used to generate threat and vulnerability alerts and to inform the public and private sector threat-hunting and incident response communities.

## **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?**

FOCI risk mitigation requirements are generally easy to incorporate into broader enterprise risk assessments and cyber maturity model evaluations since most of the FOCI-required technical, physical, and administrative (or management) controls are widely recognized or otherwise accommodated within common information security and risk management standards and guidance, such as the ISO/IEC 27000-series, NERC-CIP, National Institute of Standards and Technology Special Publications, the Center for Internet Security Top 20 Critical Security Controls, and others. Additionally, while not always incorporated into an enterprise risk assessment, corporate governance and its role in cyber risk management should be a feature of risk assessments and evaluations of an organization’s cyber risk management program. NAIS recently develop a Cyber Risk Management Program schema, based on common standards and guidance, and an associated evaluation that would capture the roles of an organization’s board of directors and other senior leadership, including those mandated as FOCI mitigations.

To the extent trusted hardware, software, and firmware profiles are available for critical electric infrastructure components, regulators might consider guiding or requiring, as necessary, that owners and operators of critical electric infrastructure incorporate such information into supply chain risk management practices that are part of a broader cyber risk management program. Of particular interest would be correlations between foreign ownership, control and influence, or FOCI, concerns and observed deviations from trusted profiles within infrastructure components.

---

As such, a reporting mechanism that enables the federal government to receive observed deviations for specific components would be useful.

### **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 of Energy can take two facilitating actions to support responsible and effective private sector procurement practices. First, the Department can support private sector entities in the maturation of their approaches to supply chain risk management. This could include working with the National Institute of Standards and Technology to continue developing and refining sector-specific applications of the principles contained in NIST SP 800-161 (Supply Chain Risk Management Practices for Federal Information Systems and Organizations). This could take the form of guidance, model policies and processes, and conceptual approaches to integrating supply chain reviews with procurement activities. Such materials would need to be tailored to the unique circumstances of an adopting private sector entity, but they would support the integration of cyber supply chain risk considerations with procurement operations.

On their own, however, these practices and guidance are insufficient. They require the inject of information so that an entity can make informed decisions. While some of that information will be sourced from within a private sector entity, much of it needs to be captured externally. The Department should identify ways by which a consuming private sector entity could ingest threat and vulnerability information from the various threat information sharing and vulnerability disclosure channels already established by the Department, the Cybersecurity and Infrastructure Security Agency, law enforcement, the intelligence community, the private sector, and academia. Individual entities often lack the resources to collect the information that can enrich even a well-developed supply chain risk management and procurement practice. The government already obtains much of this information and maintains programs to share it. If government wants industry adoption of better, risk-informed procurement practices, it should reduce those barriers where it has the capacity to do so with little cost to the government/tax payer.

### **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?**

As previously suggested, the Department could support the mitigation of foreign ownership, control, and influence risks, in addition to other sources of supply chain risk, through the development of trusted hardware, software, and firmware profiles. In addition to other threat and vulnerability information that can be made available by the government, these profiles would enable utility procurement policies, state requirements, and FERC mandatory reliability standards to incorporate the concept of “known-good”. Too often, the security community applies detection approaches centered on identifying known or suspected malicious or vulnerable activity, hardware, and software. While this approach enables the application of previously generated knowledge, it does not address the continuous introduction of new threats and vulnerabilities or variations on prior observables. Thus, the community is faced with an

---

unbounded problem space. Through the introduction of trusted profiles, the Department can bound the problem space and solve for known-good.

F2 Tvslnfrmsr{Eylsvx}\$

**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?**

A Prohibition Order needs to weigh the needs of utilities to procure and deploy equipment in support of the services they offer with the need to do so in a safe and secure manner. If the Department can support utilities in better delineating the risks associated with different equipment and/or suppliers, then a Prohibition Order may be appropriate for equipment or suppliers that are observed to exceed documented risk thresholds.

**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?**

Any Prohibition Order should take into account the dependencies and interdependencies within U.S. critical infrastructure. While a Prohibition Order is regulatory in nature, the Department would benefit from analysis and feedback obtained via the voluntary framework governing collaboration between the federal government and critical infrastructure sectors. Specifically, the relevant sectors' Sector Coordinating Councils, Government Coordinating Councils, and Sector-Specific Agencies should have an opportunity to inform the Department's Prohibition Order calculus. In addition, the Department should consider coordinating its analysis with the Cybersecurity and Infrastructure Security Agency's National Risk Management Center (NRMC) to obtain dependency analyses conducted by the NRMC and the national labs on its behalf. Such Prohibition Orders may be appropriate, but unintended consequences should be researched and understood in advance.

**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?**

Please see the response to Question #2 above. It applies to critical infrastructure and national critical function considerations.

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

Our experience is that the ability of utilities to identify critical infrastructure within their service territory is case-specific. The Department, working with the Cybersecurity and Infrastructure Security Agency, should partner with SLTT governments to devise an approach for sharing what



---

federal and SLTT governments know about the identities of critical infrastructure within specific jurisdictions. This may involve government encouraging critical infrastructure to self-identify in contracting or other communications avenues with their relevant utilities. The information is available, but an efficient process just needs to be established that enables it to be shared in a manner that does not add risk to critical infrastructure entities and that does not discourage preexisting voluntary participation with federal and SLTT critical infrastructure initiatives.

## **CONCLUSION**

Once again, we at NAIS and Eclipsium encourage the Department of Energy's efforts to bring better risk management and security to the nation's critical electric infrastructure. While much in cyber risk management and security depends on good governance and processes, the role of technical solutions cannot be overlooked, especially when there is a need to scale situational awareness of component and service supply chain risks and other vulnerabilities. When those risks emanate from deep within often-overlooked hardware or firmware, Eclipsium's currently available commercial offering provides a scalable means to achieve the needed awareness, which can be considered within NAIS's continuously evolving risk management approach. We are excited about opportunities to support the U.S. Department of Energy's emerging risk management requirements, and we are confident that, given the resources and partnerships we have built for opportunities like this, that our team would provide unmatched levels of performance, service, and responsiveness. We hope our responses assist the nation as it addresses this important national security matter, and we are prepared to submit any additional information that you might find useful. Thank you once again for the opportunity to provide a response.