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

Send Via EMAIL: ElectricSystemEO@hq.doe.gov

Comments of Baylor University:

Security of the United States critical electric infrastructure is a topic that affects every American and, as such, should be within the interest of all. The commoditization and reliable access to electric infrastructure have defined the American way of life and, without a nationwide effort, could be our greatest weakness. We applaud the Department of Energy for investigating new ways to secure the grid more effectively. As Secretary Granholm recently stated, "It's up to both government and industry to prevent possible harms -- that's why we're working together to take these decisive measures so Americans can rely on a resilient, secure, and clean energy system."

Chief among the measures we need to address is the concept of true resiliency. While resilience certainly includes securing systems from compromise by anticipating and resisting attacks, we simply cannot stop there. Instead, we must prepare our electric infrastructure to continue operation despite failure of components and security. To do this, we must prepare the grid to adapt to new conditions and recover from failure.

Numerous vulnerabilities and threats challenge the viability of such resilience, including:

- The patchwork of infrastructure ownership and operation makes it difficult to implement a consistent policy on infrastructure maintenance, monitoring, security posture, etc. The fires caused by aging electric infrastructure and the resulting bankruptcy of PG&E demonstrate that market force and national priorities might not always align.
- Lapses in infrastructure ownership and supply chain provenance have led to an untrusted electric infrastructure. The recent SolarWinds incident highlights that supply chain risks are not only from foreign supply companies but also from adversaries compromising domestic companies.
- It is well-known that foreign adversaries are actively working to infiltrate electric distribution control systems to enable compromise at an opportune time.
- A non-trivial portion of the current electric infrastructure operates over components and systems provided by companies under the governance of US adversaries.
- New technologies in both the consumer (e.g., renewal energy, electric vehicles) and commercial (e.g., Internet-connected industrial control systems) space creates pressure for rapid transformation of the infrastructure, for which there has been little or no time for evaluating the security implications. It is now common for remotely controllable, IoT devices such as thermostats to be operating household units. Even worse, consumers are financially incentivized to connect their untrusted IoT devices directly with grid operators (e.g., temporarily turn off A/C units during peak demand to smooth power consumption).

Several recent incidents demonstrate the fragility of our current electric infrastructure. The news about the failures in the US electrical grids has certainly not escaped the notice of US adversaries. The Winter Storm of 2021 shows just how fragile that critical electrical infrastructure

can be. ERCOT reported that the Texas power grid was "4 minutes 37 seconds away from a total collapse," which would have caused a blackout in Texas for weeks if not longer. Such failures may have severe consequences for national security. Texas is home to 15 military bases, all of which rely to some degree on the local grid infrastructure to maintain operational readiness. Texas is home to the largest active-duty deployment of Army and Airforce in the United States. The National Center for Policy Analysis has said that "Even with the Military's most advanced stand-alone microgrids and emergency recovery systems, federal installations in Texas remain reliant on the grid. An EMP attack and the subsequent, prolonged blackout has the potential to not only devastate America's military capabilities, but *permanently undermine U.S. national security."* We have the perfect storm of vulnerable electric infrastructure, public exposure of this to our adversaries, and a dependency of military readiness on that infrastructure makes the evolution of our infrastructure a clear and pressing national security concern.

The SolarWinds hack conclusively demonstrates the effectiveness of supply chain compromise as an attack vector and the willingness of state actors to employ this approach. Attacking the roots rather than branches provides the best approach to killing a tree. This sophisticated attack circumvented traditional identification steps, such as known indicators of compromise, and was accomplished by inserting malware into the development cycle of relatively benign IT management provider. As a result, the hackers "successfully compromised about 100 companies and about a dozen government agencies. The companies include Microsoft, Intel, and Cisco; the list of federal agencies so far includes the Treasury, Justice, and Energy departments and the Pentagon." The SolarWinds attack on our electric infrastructure even compromised the Cybersecurity and Infrastructure Security Agency (CISA), the very agency tasked with mitigating these types of attacks. And most recently, the Colonial Pipeline attack showed how advanced persistent threats (APTs) from peer and near peer countries can wreak havoc on the energy sector in a rapid timeframe. The pipeline, which transports gasoline, diesel, jet fuel and other refined products from the Gulf Coast to Linden, N.J., was shut down for six days. The stoppage spurred a run on gasoline along parts of the East Coast that pushed prices to the highest levels in more than 6 ½ years and left thousands of gas stations without fuel. As Colonial prepared to restore service, its personnel patrolled the pipeline searching for any signs of physical damage, driving some 29,000 miles. The company dispatched nearly 300 workers to keep their eyes on the pipeline, supplementing its usual electronic monitoring. This underscores the unique cyber/physical security concerns over grid protection as the ever-evolving battlespace of cybersecurity moves more towards kinetic end-states.

Undoubtedly, the critical electric infrastructure in the United States is a core component of US national security. However, securing this infrastructure is not a simple task and will require the input of local and national government, industry, academics, national laboratories, and other stakeholders. We propose that **the solutions to securing our critical electrical infrastructure must be more than technical or policy in nature**. Techno-policy may in fact only address the symptoms of a much deeper issue in the US, the siloing of our academics, government authorities, private industry, and defense departments. These silos, something notably absent in unitarian states such as China, dramatically restrict the speed of innovation.

Innovation has long been recognized as a critical component to the meteoric rise of the United States as a world power. However, strategic and focused investments by peer nations are rapidly closing that gap. China threatens the U.S. leadership in science and technology for the first time since the end of World War II. According to the Council on Foreign Relations "There is a great deal of talk among policymakers, especially in the Defense Department, about the importance of innovation, but the rhetoric does not translate fast enough into changes that matter." Authoritarian governments have learned to utilize their form of government to accelerate R&D efforts in science and technology to great effect and copying such a model in the U.S. would be an affront to the very ideals on which our nation was built. As such, **a uniquely American approach to accelerating innovation should be encouraged by the Department of Energy.** Such an approach would leverage the creativity and expertise of our world-leading academics, the resources and competitive nature of domestic industry and utilities, and the best practices already developed by our intelligence and defense agencies.

A complex set of factors contributed to the highly vulnerable state that currently exists, including untrusted suppliers, devices, networks both in the electric infrastructure and at the endpoints; lack of sufficient security in products from any vendor; lack of sufficient workforce to design, develop, procure, configure, operate, and maintain cyber-enabled infrastructure. Any solution must recognize that this problem, which has been decades in the making, cannot be fixed overnight.

In order to implement the envisioned solutions, a consortium of stakeholders is required, with the required expertise to address the myriad and evolving challenges we face. Baylor University is a trusted, independent broker bringing together and managing many diverse entities required and ensuring successful near-term, mid-term and long-term solutions. This unique consortium fosters strong partnerships between Government, Industry, and Academia to assist the DoE in a host of efforts, including:

- Building an inventory of critical electric infrastructure
- Constructing the threat models and risk analyses for our current and evolving infrastructure
- Identifying the priorities for infrastructural improvements based on the risk analysis
- Explicitly defining our supply chain, including hardware and soft/firmware, and interdependencies
- Confronting the issue of installed, untrusted components of the electric infrastructure
- Designing for resilience with graceful degradation instead of purely relying on prevention

Furthermore, we encourage the Department of Energy to consider the *speed of innovation* and *variety of defense* as critical components required in addressing the continually evolving threats.

Our team seeks to bring together a wealth of expertise to help the DoE protect the Nation's critical electric infrastructure, including leading industry, academia, and DoD Prime integration expertise combined with best of breed technology providers. Our team also includes a number of energy sector companies, including some of the largest, that are aligned with our strategy and understand the importance of the issues we are addressing:

> **Baylor University:** Baylor University is launching a large-scale project we refer to as the Baylor Cyber Range and Research Complex (BCRRC) as part of a larger $1 billion+ capital

campaign. The BCRRC will act as a best-practices testbed for our industry partners as well as a talent development pipeline and substantial cyber research facility for academia, industry, and government. We believe that Baylor can serve as an innovation hub to tackle these large-scale and interdisciplinary problems. Baylor's Lab to Market (L2M) collaborative and significant cutting-edge research is well suited to these challenges. Our ability to fuse the technical and non-technical areas of research, from science to policy to economics and beyond, can be a real resource for the Department of Energy as it seeks to better understand and respond to the emerging asymmetrical threats to the grid that cyber represents. In addition, Baylor has pulled together a substantial and multi-faceted team that can bring together the resources and skills necessary.

L3Harris: One of the largest defense industry primes, L3Harris is a trusted cybersecurity partner with two decades of cybersecurity experience. L3Harris incorporates modern cybersecurity protections, defense-in-depth techniques, least privilege, redundancy, industry best practices, Standard Technical Implementation Guides (STIGs), and innovative security approaches into the mission system as a critical core function of the architectural design. The DoDD 8570-01m-qualified L3Harris Cybersecurity Team uses Risk Management Framework (RMF), Cyber Survivability Endorsement (CSE), and System-Theoretic Process Analysis for Security (STPA-Sec) to assess the overall cyber risk and abatement of infrastructure in accordance with FISMA, DODI 8500.01, DODI 8510.01. As with the functional requirements, we use Model-Based Systems Engineering (MBSE) tools to instantiate attack surfaces, threats, attack trees, risk analysis, and cyber requirements. RMF and CSE methodologies are applied for each sub-system in the architecture. Attack surfaces are identified for individual sub-systems and correlated to threats and attack goals.

L3Harris uses these analysis techniques for overall assessment of DoD and other sensitive customers' platforms. We routinely assist and coordinate accreditation and secure Authority to Operate (ATO) for equipment installations on secure DoD networks, including cyber testing and supply chain risk management as required. Leveraging this experience for DoE installations and equipment will result in rapid hardening and robust securing of our nation's infrastructure and assets.

Conxx: GridObserver® by Conxx is a full-service network management framework that works by looking widely (across many vendors WiMAX, Microwave, Switches, Routers, etc.) and deeply (into the MPLS/ATM/SONET/Routing/DWDM) layers of the network. Monitoring using GridObserver® takes into account not just physical devices and connections, but the virtual aspects that exist within and without any discrete device on the network. GridObserver currently manages all Exelon Opco's and "adds a 9" to every network it is added to.

BTU Research: BTU Research works on Smart Grid Programs for Tier 1 Utilities. To ensure this continuity of data from the many IoT Edge devices, utilities use BTU SolidSwitches to enhance grid network resiliency. Unlike legacy industrial switches, which do little more than provide power and move data, the SolidSwitch is an integrated

Network Platform designed specifically for the Edge. Network switching is combined with remote intelligent power, data center quality UPS, emergency Li-Ion storage and redundant wired and wireless communications. This integrated Network Platform operates in the most extreme environmental conditions. Packaged in a 9”x 11”x 7” hermetically sealed, hardened enclosure, the unit withstands hurricane conditions, operates at temperatures from -35º to 160ºF. Operational resilience requires the ability to prepare for, withstand & recover from compromise resulting from attack, infrastructural failure, or natural disasters. SolidSwitch is a proven Network Platform that provides resilience to any Critical IoT requirement.

Wind Talker Innovation: Osmosis security begins with network discovery and network entry. Osmosis is designed to automate and integrate these processes by utilizing encryption certificates as its checksum for completion. Once a device has securely entered the baseline network, each message sent is encrypted for security to ensure all communications are secure end-to-end regardless of the data path selected, even when using commercial networks.

In addition to securing network entry, messaging, and data paths, WTI has also created a Multi-Level Security (MLS) architecture that involves seamlessly encrypting subnets and user groups that can be restricted by any number of modular criteria (e.g., Whitelist, Blacklist, username/password, biometrics, server, geographic area, etc.) that can be modified for mission security and speed. These criteria can be set in any configuration. Network Operators could stipulate that only whitelisted devices within the AO, that have biometrics from a wearable connected to the approved device, will be permitted. Moreover, because it is modular, any other technology available can easily be added to the schema. Most importantly, the network does not fracture when multiple layers of security are applied, this is extremely unique for an ad-hoc mesh network. WTI is the only networking company to do this, and it is patented. The Osmosis subnets allow MLS throughout the architecture, by creating the ability to seamlessly transition between subnets, and issuing Over-the-Air (OTA) certificates in real-time, as situations change and modifications to network access need to be accomplished. Access can be managed autonomously or by an Operator-In-The-Loop. Since Osmosis is simply software that loads onto devices, it can be employed in any device or platform and, with OTA updates, can be installed or updated in any environment. This construct enables interoperability and alleviates posse comitatus and LE sensitive issues when sharing information across networks.

Communication Security Group: Global leader and innovator in Secure Mobility, operating at the intersection of cybersecurity and mobile and desktop communications. CSG offers the next-generation of messaging and voice apps for secure, trusted mobile and desktop communications, that allow anyone to carry out real-time, end-to-end encrypted calls, with crystal-clear voice quality, and exchange messages and documents between devices, around the world.

Through decades of experience in government, military, and the private sector, CSG has created a suite of products that addresses the needs of both organizations and their end users. CSG's communication security platforms, operate seamlessly across iOS, Android, Blackberry, and PBX systems, and are suitable for any organization regardless of size. CSG provides government-grade encryption levels for organizations that demand the strictest security requirements with flexible pricing for smaller enterprises seeking an affordable communications privacy solution. And with its ultra-low bandwidth requirements, operate in a carrier-agnostic manner across IP connections from 2G Edge to 5G.

Response to Specific Questions

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

States, Indian Tribes and units of local government need to implement the core goals of cyber resiliency relative to the electric system. The core goals of cyber resilience as defined by NIST[1] are: anticipate, withstand, respond to, and adapt to adverse cyber conditions. In order to achieve each of these goals, these government entities need assistance with the following:

- Workforce Awareness and Development: States, Indian Tribes, and local governments need educational programs in their locales to foster awareness of cybersecurity issues in the workplace and in the development of a cybersecurity workforce. Colleges, universities, and trade schools are well-positioned to fill this need to train future leaders and practitioners in the field. Support for these training organizations not only includes financial, but also internship opportunities, data-sharing partnerships, and workshops, to name a few. Not only should this be emphasized for post-secondary education, but also for K-12 programs, as well. For example, summer camps that educate students on the importance of cybersecurity and the power grid will be crucial for recruiting the next generation of cyber defenders. All students and even practitioners should be encouraged to participate in cyber challenges. In addition, domain-specific challenges should be developed for all levels of participation. The workforce needs to be trained in areas such as: network security design, network security analysis, cyber incident response, and system hardening among others.

- Assistive System Monitoring and Mitigation Planning: States, Indian Tribes, and local government units may be unable to quickly transition from untrusted components and may not have qualified personnel for securing untrusted/trusted components and infrastructure. They can benefit from an organization tasked with 1) regular security testing of local electric distribution infrastructures, 2) reporting results to stakeholders, and 3) providing remediation instructions/assistance.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

- Prescribe Zero/Limited Trust Best Practices: Zero trust is quite frankly an overused buzzword these days without the requisite remediation behind it in many cases. The foundation of zero trust is identity. Implementing proper Identify Credential Access Management (ICAM) and other measures is critical to properly identify both the people operating every device and the devices themselves. States, Indian Tribes, and local government units often lack the in-house expertise on security electric distribution infrastructure. Complicating the matter further is the fact that components are likely to be untrusted and lead to unknown outcomes. Therefore, governments need to shift to a "zero trust" model where explicit trust is granted after suitable evidence is provided to merit trust. This will likely require the establishment of practices that assume a breach has occurred. Governments can benefit from published Standard Operating Procedures (SOPs) and industry best practices guidelines to deal with isolating untrusted infrastructure and making update/transition plans for equipment from a trusted supply chain. These guidelines must then be regularly practiced by Governments to ensure that the workforce can respond properly when an incident occurs.

- Operational Cyber Incident Response: States, Indian Tribes, and local government units may lack a tiered incident response organization so that there is a prioritized incident handling and response for Energy sector cyber compromises. This organization would require transparent, timely reporting of cyber incidents and provide the infrastructure to determine and take the appropriate action. For example, with the Colonial Pipeline cyber incident, this organization would be responsible for coordinating, determining, and executing a response best in the national interest, rather than relying on a single corporation to respond.

- Research and Development: States, Indian Tribes, and local government units all need tailored, context-aware strategies and approaches to address their security needs. In order to get solutions that are relevant to them, these entities need better partnerships with the research community. To accomplish this partnership, the Department needs to better coordinate research with other Government and academic entities. While funding is something state governments should allocate resources towards, there are additional ways to support the research and development community that these government entities should be pursuing. In order for the research community to deliver relevant solutions, they need realistic, representative system and network data, which Governments can provide reference data sets to the community. Additionally, Government entities can provide example scenarios for researchers to utilize for their threat models when developing new solutions and capabilities.

- Supply Chain Monitoring and Evaluation: Attacks like SolarWinds highlight the fact that supply chain threats can be stealthy and far-reaching. With the global economic marketplace, it is imperative that Government entities have the ability to monitor and evaluate the supply chain. In order for this function to exist and be successful, a number of things are required. First, the development of criteria that can be utilized in evaluating

a supplier/vendor, as well as specific technical criteria for evaluating a specific component or technology. Second, independent entities will evaluate suppliers and components and digitally publish those findings in a manner that is easy to access (e.g., website). As CMMC moves beyond DoD and into civilian agencies, the Department should look at ways to improve the underlying architecture of CMMC and glean best practices, while also avoiding the areas that industry has kicked back against a perceived heavy-handed approach to government oversight.

- Trusted Independent Evaluation Organizations: Many government entities lack sufficient people to be able to evaluate the cyber resiliency of their solutions or to implement them. Therefore, it is recommended that criteria for independent evaluation organizations be developed and then to identify those independent organizations. These trusted independent organizations should be not-for-profit, non-profit, or academic institutions who are not motivated by potential profit, but rather are able to provide a trusted, independent assessment of a design or implementation.

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?

To address the security of critical electric infrastructure, the Department should evaluate security designs by encouraging designs based on a zero/limited trust model. Additionally, when evaluating the design of the critical infrastructure, the critical components need to be explicitly identified and designed and integrated such that, if a supply chain threat is realized, the cyber impact is mitigated. Therefore, the system design should be resilient (able to anticipate, withstand, respond to and adapt to cyber threats) and should include, but is not limited to, the following:

- Network segmentation and controls that enable the ability to isolate identified compromised components on demand
- Identification of known good network traffic/behavior at design and implementation time
- Monitoring of existing infrastructure for compliance with best practices
- Providing expert advice on migration to/adoption of best practices based on specific requirements/context
- Network and system anomaly monitoring
- Hardware/firmware/software modification monitoring – often components exist in physically unsecured locations. Therefore, there needs to be a way to monitor changes to those components' hardware/software/firmware.

- Cyber incident response capabilities (semi-automated, human-assisted)

- Fully encrypted data-in-transit with proper controls over each end-point within a zero-trust architecture

In addition to security design evaluations, third-party security testing and supply chain pedigree testing should be conducted. Security testing should be performed by qualified penetration testing teams specialized in these efforts. This is likely done to some extent currently, but prior to these engagements, there should be threat scenario planning and development that aids in penetration testing. Testing should move beyond tabletops and red/blue team exercises to a full Rehearsal of Concept (ROC) drilling protocol that tests the various unknowns of any real -scenario. By forcing response teams to physically respond and deal with the real-world realities of travel-time, missing equipment, etc., the Department can improve readiness. Tabletops are simply insufficient for critical infrastructure crisis response and mitigation. Lastly, each critical component should be evaluated by an independent third party for malicious supply chain attacks.

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?

In order to facilitate responsible and effective procurement practices, the Department needs to have initiatives related to the three main ways security issues are introduced into systems. These issues arise from defects in 1) the things we buy (e.g., COTS), 2) the things we custom build (e.g., software), and 3) the way the components are put together/integrated (e.g., configuration errors). The following are some things that the Department can influence in order to facilitate responsible and effective procurement practices:

- Software and Hardware Assurance: The Department needs to levy requirements in their contracts that require vendors to provide the Department with the following information related to Software and Hardware Assurance: a) identify assurance tools employed (including configuration of tools), b) results of tools employed and how those results impacted the design, development and testing c) results for both custom developed and Free Open Source Software (FOSS). In addition to requiring the data, the Department should provide metrics of sufficient assurance and quality of the software and hardware in their supplier contracts to ensure that sufficient assurance is provided.

- Develop Testing Labs: Develop national laboratories that can provide a combination physical/virtual emulation environment that allows for testing of individual components, as well as systems that mimic the integration in the field. Such a lab can enable 1) student/practitioner training on high-fidelity approximations of real-world conditions, 2) researcher access for exposing flaws and developing responses, and 3) an industry collaborative on improving system resilience. These labs can exist in academic research

institutions with government, industry, and academia working under one roof to solve complex problems.

- Develop Criteria and Evaluation Process for Supply Chain Pedigree: Common Criteria has flaws in its approach, but there are elements from it that could be effective for evaluating Supply Chain issues. The Department could define a process and metrics for evaluating the supply chain pedigree of a specific vendor and also of specific vendor solutions. They could then identify trusted third-party entities that would be responsible for evaluating the pedigree of vendors and their solutions that could be publicly available for all to review when making acquisition decisions.

- Develop Secure Development Environment Requirements and Evaluation Criteria: The SolarWinds incident has taught us the importance of a secure supply chain. The Department should levy requirements on acquisition contracts for a sufficiently secure development environment. Sufficiency would need to be defined for different types of components or solutions being developed. Additionally, a process and set of criteria to evaluate and monitor the implementation of secure development environments would be needed to ensure not only the initial instantiation of a secure development environment, but also that the environment maintains sufficient security controls in place throughout the development process.

- Increase Workforce Development Initiatives: Partner with colleges, universities, and trade schools in creating training programs that do not require four year degrees, but certificate programs to rapidly enable the training of the workforce in key areas such as network security design, network security analysis, cyber incident response, and system hardening among other areas. Additionally, target the development of camps and summer programs that are designed for educating and recruiting underserved populations for cybersecurity and the energy sector.

- Fund Research and Development for Secure Integration and Supply Chain Pedigree Evaluation Tools: Acquisition programs that are developing and acquiring solutions need a toolset that they can utilize in order to determine whether to accept a solution or not. This toolset would need to be able to evaluate whether a solution has secure integration of its components by being able to quickly develop threat scenarios and measure a system's performance against those threat scenarios. Additionally, the toolset should be able to scan the source code and the configurations and test the security of the integration of all software/hardware components. Beyond secure integration, the Department should also be funding the research and development of tools and processes to be able to measure the pedigree of the supply chain and the threat it poses to the system, as well as the mission the system supports.

- Enable Collaborative Resilience: Reliance on security to guarantee operational continuity is doomed to fail. Successful solutions include systems capable of graceful degradation

and a response from heterogeneous systems so that a single vulnerability is unlikely to compromise all layers of defense. As electric distribution infrastructures are naturally localized and distributed, they provide an excellent opportunity for the utilization of edge computing and communication in response to a compromise event. Systems can be built to collaboratively respond rather than simply react and hope in isolation.

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?

The problem is worthy of a research program that the Department should fund. However, NIST recently released NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: Observation from Industry which identifies 9 key practices. For each of these practices, the Department could develop specific criteria to evaluate whether these practices are sufficiently being implemented. The 9 key practices from NISTIR 8276 and some possible example metrics (but that need more specificity to make them measurable) are:

- Integrate C-SCRM Across the Organization
  - Are key stakeholders (e.g., procurement/supply chain, information technology, cybersecurity, operations, legal, physical security, enterprise risk management) active participants in SCRM
  - How often do the stakeholders meet
  - Do the meetings address the key functions needed for SCRM: evaluate risks and risk mitigation plans, set priorities, sharing of best practices, etc.
  - How often is the criteria reviewed and updated
- Establish a Formal C-SCRM Program
  - Is the SCRM Program chartered and supported by senior management
  - How often are the charter and guidance reviewed and updated
  - Maintenance of an Approved or Banned Suppliers List (and how often is it reviewed/updated)
  - Use of escrow services
  - Documented list of alternative sources of critical components (and how often is this list reviewed/updated, how is accuracy measured and maintained)
- Know and Manage Critical Components and Suppliers
  - Documented component and supplier dependencies (how often is this list reviewed/updated, how is accuracy measured and maintained)
  - Documented list of critical components (how often is this list reviewed/updated, how is accuracy measured and maintained)
  - Documented metrics and analysis for identification of critical components
  - Risk the supplier provides to the organizations network infrastructure (does the supplier have access to the organization's network and networked assets)
  - Risk calculation of supplier being a threat vector to the organization

        - Documented Risk Mitigation Plan for critical components/suppliers (how often is this list reviewed/updated, how is accuracy measured and maintained)
        - Documented list of alternative sources for critical components/suppliers (how often is this list reviewed/updated, how is accuracy measured and maintained)
        - Network segmentation controls for critical components
- Understand the Organization's Supply Chain
    - Degree of visibility into supply chain of outsourced manufacturers
    - Is the visibility real-time (how often is it updated)
    - Software and hardware inventory exists (and how often reviewed/maintained, how is accuracy evaluated, what is the accuracy of the inventory)
- Closely Collaborate with Key Suppliers
    - Frequency of interactions with suppliers
    - Roles in organizations interacted with
    - How often site visits/inspections are conducted
    - Are the regulators rotated between sites so that the same individual is not always auditing the same set of suppliers
- Include Key Suppliers in Resilience and Improvement Activities
    - Process and protocol for sharing vulnerabilities and incidents
    - Clearly identified responsibilities for responding to cybersecurity incidents
    - Documented Lessons Learned (and process for collecting lessons learned)
    - Regularly reviewed and updated response and recovery plans
- Assess and Monitor Throughout the Supplier Relationship
    - Monitor the component for anomalous behavior
    - Documented Supplier Assessment at the beginning of the relationship
    - Documented requirements, controls, and mitigation adjudication process
- Plan for the Full Lifecycle
    - Tracking database of end of life or end of support for each component
    - Regularly reviewed database for high-risk components
    - Mitigation plan documented for any high-risk component

See NISTIR 8276 for a more complete list than the examples above.

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?

We recommend the Secretary order development and implementation of an infrastructural transformation plan designed to rapidly secure national infrastructure. Just like the nation needed a bold vision during the Space Race in an aggressive timeline, a similar approach is needed to secure national infrastructure. Such a plan must consider factors like supply chain availability,

national security and economic priorities, and financial/construction capabilities. The plan should consider the following in priority order.

- Develop isolation and monitoring strategy and practices for existing infrastructure. Provide utilities with a service for controlled trust of external interactions such as communication with manufacturers, soft/firmware updates, etc.

- Inventory electric distribution systems, identifying those whose compromise would have the greatest national security, critical infrastructure, and economic impact.

- Develop a distribution system security transition strategy that takes into account national priorities, supply chain, and construction equipment/expertise availability.

- Develop a sustainable and expandable supply chain strategy and plan from identified trusted sources. Such a plan must recognize the significant cost of investment in new/improved manufacturing by making pre-purchase commitments, etc.

- Develop a strategy of orders, incentives, and penalties that compels infrastructure operators to collaboratively isolate and monitor until they can transition to a secure national infrastructure at the earliest opportunity in the rollout plan.

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?

The strategy recommended for question #1 should take electric infrastructure dependencies into account when establishing transition priorities. The rollout plan should carefully consider sector interdependencies and strategy impact, i.e., electric system modernization where the cure is not worse than the disease.

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?

Yes. Additionally, the strategy recommended for question #1 should take into account national critical functions by definition are high-impact functions and would therefore make for a higher priority target for adversaries. Therefore, electric infrastructure enabling the national critical functions should be prioritized.

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

No. The utility companies' "sufficient ability" should be evaluated in a few different dimensions. Those dimensions include: technical competence, available resources to perform investigation, available information, and incentive to identify and respond. While it is common for organizations to wish to be compliant, there needs to be external entities that, at a minimum, monitor and enforce compliance. However, it is more likely that external entities would also need to perform compliance checks and oversee implementation for certain compliance functions. Having companies self-police is unlikely to succeed as revenue drives priority and investment. Third-party evaluation with a collaborative environment for remediation along with the right incentives for participation is key to driving improvement with respect to security and resilience.