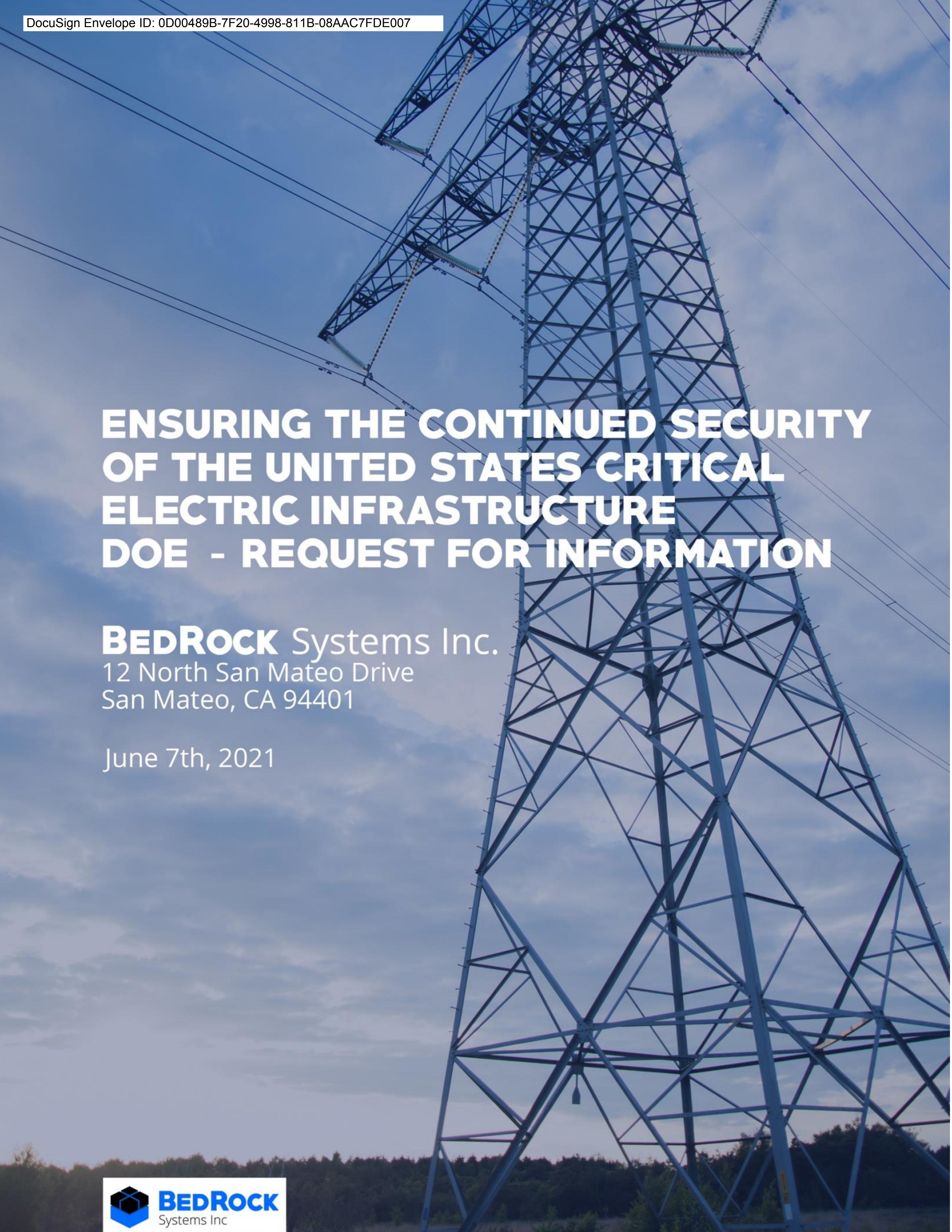

ENSURING THE CONTINUED SECURITY OF THE UNITED STATES CRITICAL ELECTRIC INFRASTRUCTURE DOE - REQUEST FOR INFORMATION

BEDROCK Systems Inc.
12 North San Mateo Drive
San Mateo, CA 94401

June 7th, 2021

BEDROCK
Systems Inc

TABLE OF CONTENTS

1.0 INTRODUCTION

BedRock Systems, Inc. is pleased to provide a response to the Department of Energy (DOE), Office of Electricity -Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure, Number 6450-01-P.

The recent ransomware attacks on the Colonial Pipeline and our infrastructure re-enforces the timeliness and importance of our response to this RFI. The dependence of over 330 million U.S. citizens on the reliable supply of electricity to perform essential functions of their daily lives highlights the sheer breadth of the impact such incidents have on our society's economic, health, and national security. It also indicates the continuous vulnerability of the U.S. electrical infrastructure to cyber-attacks and demands us to not only apply conventional approaches to address this problem but explore novel approaches to respond to this emerging threat.

BedRock Systems, Inc. is a start-up that has been founded on the principle of developing products and solutions that enable Prevention, Mitigation, and Resilience against cyber threats in the Information Technology (IT) and Operations Technology (OT) arenas.

We are staffed and supported by some of the most advanced thinkers with the sole purpose of developing a next generation cyber-security product suite. Our world class development team draws from the experience of industry experts, academic research professionals, and the understanding of federal space and its challenges.

2.0 PROBLEM STATEMENT

As described in the RFI (Federal Regishttps://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-statester :: Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure), adversarial nation-state actors are targeting our critical infrastructure, with increasing focus on the energy sector. Nation-state threat actors are equipped and actively planning to undermine the electric power system in the United States. The growing prevalence of essential electric system equipment being sourced from China presents a significant threat, as Chinese law provides opportunities for China to identify and exploit vulnerabilities in Chinese-manufactured or supplied equipment that are used in U.S. critical infrastructure that rely on these sources. DOE is seeking input to aid the Department in preventing exploitation and attacks by foreign threats to the U.S. supply chain and to ensure that the Department's considerations appropriately balance national security, economic, and administrability considerations. Accordingly, the Department expects that, during the period of time in which further recommendations are being developed, utilities will seek to act in a way that minimizes the risk of installing electric equipment and programmable components that are subject to foreign adversaries' ownership, control, or influence.

3.0 REQUIREMENTS FROM THE RFI:

Section A of The RFI, Development of a Long-Term Strategy describes high-level requirements.

A summary of the specific requirements associated with the development of a long-term strategy are;

1) Addressing pervasive and ongoing grid security risks requires a comprehensive long-term strategy,
2) Recommendations for how to best ascertain the roles of public, private, and government,
3) Ensure procurement practices and requirements evolve to match changes in the threat landscape and business requirements to best protect critical infrastructure,
4) Enable better testing and certification of critical grid equipment,
5) Encourage better procurement and risk management practices,
6) Develop a strong domestic manufacturing base with high levels of security and resilience,
7) Attention is also needed to address the challenge associated with mitigating the risks associated with potentially compromised grid equipment that is already installed, along with the expected costs and benefits of addressing such equipment,
8) The Department also recognizes innovative approaches will be needed to thwart continually evolving threats.

BedRock Systems has included a response to these requirements in Section 6 of our response.

4.0 BEDROCK RESPONSE: A. DEVELOPMENT OF A LONG-TERM STRATEGY

Many of the RFI questions are multi-part questions and comprehensive responses require addressing the individual parts of the questions to maintain context.

4.1 QUESTION 1

4.1.1. WHAT TECHNICAL ASSISTANCE WOULD STATES, INDIAN TRIBES, OR UNITS OF LOCAL GOVERNMENT NEED TO ENHANCE THEIR SECURITY EFFORTS RELATIVE TO THE ELECTRIC SYSTEM?

While the organizations currently managing the electric utilities across the U.S. have the technical knowledge and skills to install, operate, and maintain those systems, the knowledge and deep understanding of the threats and the mitigation techniques necessary to address non-physical cyber security threats varies greatly across the country.

The continuous attacks on our Department of Defense by Nation-state and other hostile actors is a prime example of cyber attack asymmetry and how difficult it is to protect deployed systems. The DoD has a tremendous investment in personnel and technology to maintain the current mitigation state, with attacks attempting to penetrating the defenses daily.

On the commercial side, the SolarWinds exploit had a 6+ month window of opportunity to exploit its victims, with many of the victims being technically savvy and actively monitoring for attacks. If an attack like SolarWinds is only caught by accident by a cybersecurity company with outstanding credentials, low profile targeted attacks against particular utilities designed to enable the takedown of entire sections of the grid are even more difficult to detect.

If the U.S. Government (specifically the DoD) and the commercial sector cyber security agencies are having difficulties finding and retaining the necessary skilled personnel to design, develop, operate, and maintains their IT and OT systems, then by extension the problem exists across the U.S.

Using the above as a proof points, the abilities of the States, Indian Tribes, or units of local government to acquire and retain sufficient quantities of the skill sets necessary to effectively mitigate the existing as well as the perceived long term Advanced Persistent Threats (APT's) will be extremely challenging without significant changes in business processes, technologies, and the knowledge of the personnel.

Technical assistance on security engineering should come in the form:

1. Creation of an independent organization similar to the National Transportation Safety Board that leverages elements of knowledge from the Cybersecurity & Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), and the Federally Funded Research and Development Centers (FFRDC) (i.e. JHU APL, PNNL, NREL, others) with a charter that would solely focus on advancing the cybersecurity initiative across all sectors of critical infrastructure. The role would be advisory and consist of the following:

    a. Creation of a clearinghouse where the States, Indian Tribes, or units of local government can gain access to qualified personnel and resources to greatly assist in building a common understanding as well as prevent / reduce the ability of companies to sell products that are either unsecure or unable to be secured – leaving the system vulnerable. (Basically, want to address the problems associated with all the Snake Oil salesmen out there who are selling panaceas that are unable to actually address the problem).

    b. In conjunction with the Utility owners/operators, States, Indian Tribes, or units of local governments create a recommended Approved Products List (hardware and software) that includes versions, patch requirements, and sunset lists - similar to what DISA provides for the DoD.

    c. Require product vendors to submit their products for validation and security testing similar to NIST Common Criteria or automotive safety testing to rate and assist with technical configurations from a security /resilience perspective.

    d. Similar to the DISA Security Technical Implementation Guidelines (STIGs) that are distributed across the DoD or automotive safety standards to support the correct types and configuration of devices/software, assist the Utility owners, States, Indian Tribes, or units of local governments in the creation and maintenance of a similar set of guidelines for the devices/software that are currently deployed across the infrastructure.

e. Implementation of a DoD Defense Industrial Base (DIB) like process where the owners, operators, and supply chain can openly share information with respect to the latest threats/breaches they are experiencing and collaborate on a community response.

f. In collaboration with Industry, establish cyber risk assessment standards/criteria that could be used in the cyber insurance and financial industries for establishing insurance premiums and cost of capital incentives based on the cyber maturity and resilience of the electrical utility.

2. Training and education to change the organizational and cultural barriers of the owners and operators required to take on some of the "heavy lifting" required to implement effective countermeasures to the threat. Due to the capital intensity and asset life cycle in critical infrastructure, there is a resistance to certain modernization initiatives due to the economics of replacing hardware/devices which constrains solutions sets and the ability to effectively secure "from/to the edge ". Furthermore, the cyber security industry continues to evolve to Security as a Service (SECaaS) forcing reliance on software overlays and monitoring/ detection. A change in the current culture via education is required for the community to implement what is necessary to meet the Presidential Executive Order's objective to pivot in the direction of zero trust and cyber resilience.

3. Consideration of economic or tax-based incentives to offset costs associated with the modernization initiatives to partially off-set the cost of more capital intensive implementations that provide higher degrees of cyber protection/resilience.

4.2 QUESTION 2

4.2.1 WHAT SPECIFIC ADDITIONAL ACTIONS COULD BE TAKEN BY REGULATORS TO ADDRESS THE SECURITY OF CRITICAL ELECTRIC INFRASTRUCTURE,

The National Security Agency (NSA), CISA, NIST and other have recently released guidelines on Zero Trust Reference Architectures that provides a comprehensive reference guide for the implementation of Zero Trust principles. These documents, in addition to the Special Publication 800-X guides published by the National Institute of Standards and Technology (NIST) and recent NIST National Cyber Center of Excellence Best Practices Guides, provides an all-encompassing road map that regulators in concert with the electric utility vendors, States, Indian Tribes, or units of local governments could utilize in the creation;

1) Utility specific best practices for the design of new products,
2) Retrofitting of existing plant, and
3) As a lever to increase understanding of the persistent threat to the utility industry,
4) Recent examples of recommended products and best practices for securing the IIoT for the energy grid.

Just like utilities in the US place a priority on planning how they will respond to a major disaster like hurricanes, floods, and earthquakes, regulators need to reinforce the need to prioritize cyber-threats as the equivalent of major disasters.

The regulator and regulations need to focus both on the prevention and response aspects. The asset owners and operators need to understand that prevention and mitigation of cyber incidents will require them to re-assess their current way of doing business. The changes to business will be on people, process and technology aspects. People will need to be trained with the right skill set. Legacy businesses processes should be revised, and obsolete (vulnerable) hardware and software will need to be re-assessed with an eye towards cybersecurity and a roadmap to modernization and mitigation of all vulnerable technologies be defined and implemented.

Regulators could require all executive level employees as well as BOD to attend a yearly TBD duration on-line educational course that provides insights into the threats over the previous year and the impact (actual or potential). Courses should be developed and presented by a group of cyber experts drawn from NIST, NSA, DOE, and Industry. The goal of the course would be to heighten the awareness and understanding of the threat, the changes that are occurring, and the need to re-enforce cybersecurity priorities within their organizations.

The derivative or flow down of this action could also include yearly threat and countermeasures training for all employees similar to other models.

Regulators could also take an action to encourage the utilities to request / require products that have more integrated cyber-security features that support Zero Trust architectures and have better supply chain pedigrees with respect to documenting the sources of as well as versions of devices and software integrated into their systems.

4.2.2 AND THE INCORPORATION OF CRITERIA FOR EVALUATING FOREIGN OWNERSHIP, CONTROL, AND INFLUENCE INTO SUPPLY CHAIN RISK MANAGEMENT,

Creation of a Federal Level policy, regulation, law that requires compliance does not necessarily assist the utilities in addressing the problem – identification of alternate suppliers (if they exist) and the entire design, procurement, installation, operation, and maintenance process takes time.

The U.S. Defense Counterintelligence and Security Agency and NIST have published extensive guidance on managing the risks associated with foreign ownership, control, and influence into supply chain risk management. This information was developed by experts in these fields, is easy to understand, and reduces the time necessary to create well structured plans, procedure, and roadmaps for the utilities and the vendors / suppliers to the utilities.

The NIST Manufacturing Extension Partnership (https://www.nist.gov/mep/supply-chain) along with the NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations SP 800-161 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf) provide excellent introductions into better supply chain management practices.

The Independent Organization referenced in Section 1 above, in concert with industry and other regulatory agencies, should lead the coordination and development of appropriate certification guidelines for the specific industry and facilitate establishment of certification bodies in the private sector.

4.2.3 AND HOW CAN THE DEPARTMENT OF ENERGY BEST INFORM THOSE ACTIONS?

While policies, regulations, laws provide high level direction, they are unable to address all the lower level unique situations that will need to be addressed. Additionally, people and organizations are resistant to change when they don't fully comprehend the necessity for the change and haven't fully bought into the change.

Ensuring the Independent Organization reference in Section 1 develops a roadmap in collaboration with stakeholders from the Utility Industry who understand the challenges faced by utilities by taking in their recommendations as well as "buy-in" to the necessary changes from the suppliers of the Utility Industry would substantially increase the credibility, trust, and acceptance of changes needed across the industry to improve cybersecurity.

4.3 QUESTION 3

4.3.1 WHAT ACTIONS CAN THE DEPARTMENT TAKE TO FACILITATE RESPONSIBLE AND EFFECTIVE PROCUREMENT PRACTICES BY THE PRIVATE SECTOR?

As indicated in Section 1 – Introduction, BedRock Systems, Inc. has developed a unique cybersecurity product for embedded controllers. As part of our sales and marketing effort to manufacturers of the embedded controllers used in the Utility Industry, we have repeatedly been told that unless there is a need for security (i.e. regulation or law), security features are not designed into products as that requires investment or increased cost which impacts margins and if the cost is passed along to the customer (i.e. price), the manufacturer is less competitive.

For years there has been a push for low priced devices – and China has been taking advantage of this by underselling all their competitors to penetrate the global supply chain, which dramatically impacts the US / European embedded system manufacturers. To remain globally price competitive, manufacturers have traditionally built-in the minimal required cybersecurity functionality in product designs as well as pushing manufacturing off-shore to low cost labor nation states like China. As a result, product features such as security and source of origin traceability have been ignored. The U.S. (and potentially other five-eye Nation States) will require standards and regulatory measures that address this issue collaborating to create a competitive market recognizing the increase in cost and price that is necessary.

Incentivizing the utilities to replace obsolete and vulnerable installed base with newer devices with self-protective features will require a change in their procurement policies and requirements. Lowest price per unit is no longer a viable alternative if the desire is to address the long term security threat to the systems. The Utilities must demand devices with the necessary security functionality, and budget appropriately as part of the procurement activities. As part of the DOE acquisitions regulations (https://www.acquisition.gov/dears) include procurement guidelines that implement standards as a requirement to meet certain criteria where the Federal and State level governments have leverage for enforcement (i.e. tax, or other financial incentives).

Beyond tracking the genesis and pedigrees of all devices, software, semi-conductors, and counterfeit devices to understand their cybersecurity risks.

The Federal Government can prioritize the requirements for securing the supply chain in the design, development, manufacturing, and procurement of the products required in addition to creating opportunities that allows the companies to design, develop, and manufacture the critical elements (HW and SW) with inherent trusted compute, identity, integrated micro-segmentation, and security features that support Zero Trust architectures. This includes establishing clear guidelines/practices for acquisition as well as software Sec/Dev/Ops and hardware manufacturing processes – securing the threat vectors in the processes we rely on for security assurance in our products.

The Federal Government should also consider the creation of financial incentives for manufacturing companies to migrate elements of these activities to CONUS – especially to Rural Area HUB Zones greater that 50 – 100 miles from metropolitan areas.

The benefit of this would be 2-fold:

1) Create jobs in areas that are still reeling from the after-effects of COVID as well as the continual sustained job losses that have occurred over the last 20 – 30 years,

2) Would move manufacturing to locations where the Insider Threat is substantially reduced – which is a key element to mitigate when on-shoring.

4.3.2 WHAT ARE THE POTENTIAL COSTS AND BENEFITS OF THOSE ACTIONS?

As demonstrated in the Russian cyber attack against the Ukranian power grid, remediation and restoration has significantly increased costs over prevention. In this case, where targeted devices on the grid were cycled to failure - the attacker succeeded not only in interrupting supply, but in creating a demand for replacement that exceeded supply thereby substantially increasing the time for full restoration.

The costs associated with not changing the way the utilities are currently doing business is un-imaginable. The Colonial Pipeline attack impacted nearly 1/3 of the U.S. population, severely impacting transportation and delivery of goods and services for a week. This along with other recent attacks in the U.S. on smart cities, the meat packing industry, and others continues to demonstrate that our traditional cyber defenses that rely on software overlays and monitoring/detection are not working – especially in the OT domain.

A similar attack to that in the Ukraine against asset owner and operators serving large sections of dense population areas for a long duration would be substantially devastating – impacting not just transportation and delivery of goods and services but also disrupting the ability of tens of millions of citizens to proceed with their daily routines with – no water, no sewer, no HVAC, no way to store fresh food, inability to cook food, no lighting, etc. It is well known that adversary Nation States have mapped U.S. infrastructure, are testing/demonstrating cyber weapons, and have likely inserted attacks that have gone undetected laying wait for the zero day. The economic asymmetry of these attacks is resulting in the proliferation of these events. We must make the necessary investments to reverse the asymmetry in favor of the defender to deter this proliferation.

The potential costs of the recommended actions are hundreds of millions of dollars over the next 20 years as obsolete or vulnerable equipment (Hardware and Software) is modernized and as the Utilities implement architectures that prioritize security features and functionality. Additionally, there will be costs associated with the education of personnel and the changes in business processes.

The long-term benefits of these actions will result in shifting the economic asymmetry of the cyber attack to the defender as a greater deterrent substantially raising the bar with respect to Nation States or rogues capable of penetrating U.S. infrastructure and include:

1) Restricting and/or disrupting the capability of the threat actors to exploit the vulnerabilities in the systems
2) Changing the culture/behaviors of the industry and community of interest with education and training on the need for cyber security along with physical security,
3) Reduction in attack surfaces that adversaries can potentially exploit,
4) Increase in resiliency to cyber-attacks,
5) Ability to recover faster,
6) One less vulnerable area of U.S. Critical Infrastructure.

4.4 QUESTION 4

4.4.1 ARE THERE PARTICULAR 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 BedRock Systems response to this question is incorporated in Question 2 above.

5.0 BEDROCK RESPONSE: B. PROHIBITION AUTHORITY

5.1 QUESTION 1

5.1.1. 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?

Attack after attack on critical infrastructure is occurring around the world - electric utilities, water & sewer facilities, energy transportation systems are just recent example from the last few years. While many of the attacks have been against equipment designed and manufactured by suppliers that don't have nefarious intentions, the threats posed by companies manufacturing equipment that have close political or economic ties to Nations or Organizations that are actively hostile to the U.S. is cause for grave concern.

BedRock Systems highly recommends the issuance of a Prohibition Order based on Intelligence Community guidance regarding procuring risk based approach for products or services from countries and manufacturers that are hostile to the U.S.

5.2 QUESTION 2

5.2.1 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 BedRock Systems response to Question 2 is addressed as part of the Question 1 response.

5.3 QUESTION 3

5.3.1. 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?

The BedRock Systems response to Question 3 is addressed as part of the Question 1 response.

5.4 QUESTION 4

5.4.1 ARE UTILITIES SUFFICIENTLY ABLE TO IDENTIFY CRITICAL INFRASTRUCTURE WITHIN THEIR SERVICE TERRITORY THAT WOULD ENABLE COMPLIANCE WITH SUCH REQUIREMENTS?

In light of the fact that the business model of most utility companies is to utilize existing installed plant elements beyond typical End-Of-Life to maximize economic Return On Investment (ROI), the installed plant spans many generations of technologies and in many cases, full understanding of the vulnerabilities associated with a particular technology (hardware or software) may not be fully known. There is also the added complexity that equipment that has been procured in the last 10 years (or so) may have embedded vulnerabilities or exploits that are ready to be activated when the time is ripe.

Additionally, organizations and companies that perform cyber-security testing as part of their business model, repeatedly discover complete understanding of installed network topologies, installed base hardware & software, and connections between unsecure and supposedly secure domains remains elusive.

Based on the above statements and the research that BedRock Systems has performed in its development of a new cyber security product, we would assert that the owners and operators of the utilities are unable to fully identify their critical infrastructure and the interdependencies across the entire critical infrastructure domain that is necessary to achieve compliance in the evolving Advanced Persistent Threat (APT) environment. While the DoD relies on organizations such as Cyber Command, NSA, and CISA – the utilities need a designated Government authority to lead this effort.

6.0 ADDITIONAL REQUIREMENTS RESPONSE

As stated in Section 3 above, the RFI Section A. Development of a Long-Term Strategy contains high-level requirements that request additional recommendations on how to proceed.

No single technology, architecture, policy, process, or procedure can adequately address the magnitude of the vulnerabilities and threats that are inherent in not only the Electric Utility sector but across the entire critical infrastructure of the United States.

There are however, some actions than can be taken that will significantly reduce the potential attack surfaces as well as mitigate vulnerabilities and threats as detailed in the MITRE ATT&CK Framework as well as the data captured in the CVE databases.

It is the opinion of BedRock Systems Incorporated that proactive implementation of the following capabilities, technologies, policies, procedures, and thought processes would substantially reduce risk and provide Prevention, Mitigation, and Resilience across the entire critical infrastructure space.

RECOMMENDATION 1: MIGRATE TO ZERO TRUST ARCHITECTURES

The leadership of Critical Infrastructure organizations must champion migration to Zero Trust architectures by using comprehensive guidelines leveraging the investments the U.S. has already made in the development of guidelines and standards.

RECOMMENDATION 2: INCREASE UTILIZATION OF IDENTITY TO ENABLE ACTIONS

While one of the key principles of Zero Trust is to authorize actions based on Identity, this concept needs to be extended down to the individual embedded device and the actions taken by those devices. Historically, embedded devices have been very limited in their abilities to execute any action they are directed to perform. Incorporating high attestation-based Identity (i.e hardware root of trust, formal methods proven unbreakable compute base, enforcement of least privilege/least functionality) at this level will substantially reduce the threat surface and enable better control of actions as well as open the door to the monitoring of device telemetry by the tools designed to detected malformed behaviors.

RECOMMENDATION 3: INCREASE SEGMENTATION WITHIN NETWORKS AND DEVICES

Implementing increased checkpoints to validate identity of and content of data flowing across the enterprise networks reduces the opportunities for unmonitored activities such a lateral movement when under attack.

As recommended by the DHS and NREL guidelines, extending the segmentation from the macro network level down to the device level – micro-segmentation between users, applications, network devices, cryptographic engine, logging, and other embedded device resources. Essentially, implementing Trust but Verify, at the lowest level – does an application require access to a resource to perform its function? Is this typical behavior for the application? Was the command to access the resource sent from an Identity that has the proper Authorization?

As part of the micro-segmentation within devices, we recommend the increased use of policies that;

1) Leverage the concept of Attribute Based Access Control (ABAC) within all end points. ABAC is an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.
2) Provide fine grain control of allow/deny lists (other related terminology includes access control, white lists, black lists) in a multi-layered defense to prevent the zero day attack based on fine characterization on least privilege/functionality on what is allowed and enforce at the compute level to constrain execution of malware instructions ("shooting ahead of the duck")
3) Use the policies and associated logging functionality to increase insights into standard vs. non-standard functionality at the end-point or embedded device to assist in macro-level analysis and detection.

RECOMMENDATION 4: IMPLEMENT AIR GAP SOLUTIONS WITH CAUTION

While a well-designed and managed Air Gap solution will provide substantial isolation and benefits, they must be designed appropriately and implemented in a way the users of the systems will not circumvent. Most organizations that rely on air-gaps have considerable investment into one-way data transfer technologies and while these technologies provide substantial value to the air-gap solution, they present the users with barriers to completion of job functions. As a result, many organizations find their expensively implemented air-gap solutions are circumvented to "get the job done" or because "the process is too difficult". There is substantial history demonstrating that air-gapping is vulnerable especially in environments where operational reliability with respect to the electric grid (especially in remote locations) relies heavily on connectivity.

RECOMMENDATION 5: CRYPTOGRAPHY

The simple recommendation is to use cryptography wisely.

Cryptography is a tool that enable higher confidence that information transmitted between source and destination hasn't been modified.

It does not mean that the information is correct and wasn't manipulated prior to transmission.

Good cryptographic implementations require that a trusted identity be at both ends of the communication path and that the actions of the users and devices are trusted to be genuine.

The final thought on cryptography is that people place too much trust on it while not understanding the strength of mechanism changes depending on a variety of implementation methods. The other concern is that at some point in the relatively near future a nation-state or a company will successfully implement a practical quantum computer that will render many of the protections that are based on cryptography vulnerable.

RECOMMENDATION 6: INSIDER THREAT, SOFTWARE, AND DATA RIGHTS MGMT

Implementing policies regarding procurement of hardware and software from nations that are hostile to the U.S. only addresses a part of the problem.

The integrity of products is also dependent on ensuring the supply chain has not been subverted via insiders (Solarwinds anyone??).

Insider threat mitigation associated with software is a multi-step process:

- Vet the employees responsible for development of software
- Code reviews / code quality / Certification and Accreditation
- Limit use of software that doesn't have a pedigree that cannot be traced to a specific owner
- Removal of unused / dead code
- Utilize Formal Methods to ensure code quality and prevent the introduction of malicious code

RECOMMENDATION 7: ANALYSIS AND DETECTION

Existing analysis and threat detection capabilities haven't been able to identify or detect emerging or deeply embedded threats. Significant investment into these capabilities will be of limited utility and generally function on a detect and respond basis – often after the damage has been done.

While essential as part of an overall strategy to mitigate repeat of similar attacks, their abilities to detect already embedded or finely crafted world class attacks are extremely limited. Even the promise of using the latest and greatest Artificial Intelligence / Machine Learning technologies will not provide 100% success as the issues with zero days is the "known unknowns". Furthermore, advanced threats include deterring machine learning and AI with false information – poisoning & mis-direction actions by adversaries who understand these technologies will increase in proportion to how extensive the deployments are to reduce their effectivity.

RECOMMENDATION 8: EVALUATION OF TRUSTED VIRTUALIZATION WITH ACTIVE SECURITY FOR MODERNIZATION/SWAP-C AND INCREASING CYBER RESILIENCE

BedRock Systems Inc. leverages the introduction of COTS multi-core 64 bit architectures such as the ARMv8 and X86. This new generation of semi-conductors with BedRock enables a formally methods proven unbreakable foundation for trusted virtualization and active security ™at the foundation of the systems being attacked. The use of trusted virtualization substantially enhances our capabilities for modernization (SWaP-C), integration, and securing our electric utility systems of systems architectures and current software applications.   Adoption of this technology by the OEM's and integrators will enhance the ability to implement a number of the recommendations listed above including: MITRE ATT&K surface reduction; implementation of zero trust per the Presidential Executive Order; "threat prevention" by constraining the execution of zero day / malware enforcing deny/allow listing policies for least privilege/functionality (and more) at the compute foundation ("shooting in front of the duck"); secure enclaves; analysis/detection ……. in both legacy modernization and greenfield initiatives. The BedRock Systems Inc. framework enables OEM's, System Integrators, and the Government to establish and deploy common reference baseline frameworks and security policies (similar to DISA STIGs) while maintaining their competitive differentiation.

Regards,

DocuSigned by:
Klaus Oestermann
595E2802D1804C4...

Mr. Klaus Osterman

CEO BedRock Systems, Inc

Klaus@BedRockSystems.com

415-845-1080

DocuSigned by:
John Walsh
519292935A454D8...

Mr. John Walsh

SVP BedRock System, Inc.

John@BedRockSystems.com

813-508-6920