Dear Mr. Coe,

Thank you for the opportunity to comment on the Department of Energy's *Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure* published at 86 Federal Register 21309 (Vol. 86, No. 76, April 22, 2021). Here are BlackBerry's initial responses to several of the challenges, concerns and risks identified in the RFI, and particularly as they relate to Part A of the RFI, "Development of a Long-Term Strategy."

BlackBerry's Perspective

In a hyper connected world, the Internet has made infrastructure more interdependent and vulnerable to cyber attacks than ever before. The attack surface of U.S. critical infrastructure is growing and becoming more complex. We have ample evidence, whether it was the SolarWinds crisis, the attack on Microsoft Exchange, the Colonial Pipeline ransomware attack, or the growing list of significant cyber incidents against State and Local Governments, that our network infrastructure is vulnerable. Traditional infrastructure used for energy, water and transportation has become increasingly connected to the Internet and must be protected. This connectivity is driven through a myriad of hardware and software – some proprietary, some open source - provided through a diverse, global supply chain. This has created a complex environment where vulnerabilities present opportunities for exploitation by malicious actors, challenges when trying to understand and manage Common Vulnerabilities and Exposures (CVEs), Common Weakness Enumeration (CWE) and the software bill of materials (SBOM), as well as appropriately responding to regulatory pressures and obligations.

BlackBerry is a global leader in embedded security solutions, providing leading edge technologies that secure critical infrastructure and the software supply chain (such as BlackBerry Jarvis) and technical subject matter experts. We have over 40 years of experience building reliable and safe embedded system software. Our operating system resides in 200 million vehicles worldwide and we work with governments globally to ensure their critical infrastructure is safe and secure.

A. Development of a Long-Term Strategy

BlackBerry is on hand to support in the development of a pragmatic cybersecurity strategy for U.S. critical electric infrastructure that is appropriate, measured and takes into account resources, expertise, risks, and threat landscape. The strategy should include risk assessment tools tailored for critical electric infrastructure operations, to help evaluate the current level of cybersecurity risks and prioritise remediation steps. Part of the long-term strategy should be a clear definition of risk appetite, ensuring periodic audits are carried out, validation of findings through technology-based assessments (e.g. verifying findings through binary scans), the development and roll-out of training and awareness, simulations and drills, as well as ensuring decision makers, budget influencers, stakeholders and the wider public are kept appropriately informed, invested in the strategy's long-term success and continuous improvement.

Naturally, the development of a long-term strategy provides a forward-thinking view of security. However, it is equally as important to ensure legacy systems, architecture, software and contracts are investigated for any potential vulnerabilities and protected. The legacy hardware and software components have often been manipulated to enable wider connectivity than they were originally designed for. This manipulation can lead to unknown risks and vulnerabilities which must be addressed – a concern highlighted by President Biden's recent Executive Order 14028, Improving the Nation's

Cybersecurity, and particularly Sec. 4, *Enhancing Software Supply Chain Security*. The Executive Order correctly notes that "[t]he security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions" and that "the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software." The software supply chain involves a complex web of dependencies with numerous third-party developers and components. In many cases, critical infrastructure operators have little knowledge of the software components that are embedded in their control systems. Securing the software in our critical infrastructure by enhancing the transparency of the software supply chain must be a priority issue.

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

   BlackBerry suggest the government look to achieve this through three parallel workstreams:

   1) Leverage professional services teams to develop industry-leading risk assessment methodologies, threat modelling, create policies and procedures which drive the overall governance, including routine auditing and regulatory compliance checks.

   2) Leverage technical subject matter experts who can penetration test the infrastructure, reverse engineer software, look for signs of malware, understand the limitations of the hardware tamper prevention methods.

   3) Leverage our best-in-breed technology (BlackBerry Jarvis) to perform binary scans on the infrastructure and any embedded systems. BlackBerry Jarvis has been specifically tailored for embedded and safety critical systems such as Critical Electric Infrastructure.

   Understanding the software composition and vulnerability exposure of embedded systems can be challenging. BlackBerry Jarvis was designed to analyze binaries within complex embedded systems. It lets the customer scan a complete software product for security vulnerabilities and software craftsmanship without the need for source code. It's a unique solution that not only enables the customer to identify potential issues, but also recommends strategies for the customer to remediate them. Finally, BlackBerry recommends that States, Indian Tribes, or units of local government look at incorporating technology such as malware detection, so they are assured most risks are being considered. Leveraging technology based solutions (such as binary scanning, malware detection) provides validation of the professional services work and identifies areas of concern that would otherwise remain hidden (e.g. information leakage from a binary, which could be exploited to facilitate phishing attacks).

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?*

   Alongside the development of a long-term strategy, BlackBerry would support the US government in developing a robust and accurate Software / Digital Bill of Materials (SBOM), consistent with Executive Order 14028, which would map out its supply chain in a way which allows it to understand the overall risks it faces. We suggest doing this through binary scanning

as it gives as close to a real-world picture of the software supply chain as possible and is often far easier to achieve than a traditional source code scan. Additionally, this binary scan will facilitate other areas of security work, such as penetration testing, understanding the attack surface, and identifying poor software quality within the infrastructure.

Consistent with Executive Order 14028 and its directive that the Federal Government advance toward Zero Trust Architecture, protecting critical electric infrastructure from malicious attacks also requires adopting Zero Trust principles to secure IT segment of infrastructure. BlackBerry recommends adopting a Zero Trust approach that continuously authenticates user and entity behaviour before granting access, regardless of network location. BlackBerry is a leader in AI/ML anomaly detection and cybersecurity and recommends that the US government adopt AI/ML enabled cybersecurity tools and approaches to dynamically prevent, detect and respond to cybersecurity threats. Detecting anomalous behavior early may help reduce the likelihood of compromise.

Thank you,

Ian

Ian Todd

IoT Practice Lead, Security Services
Mobile: +44 (0)7493 258263
itodd@blackberry.com
BlackBerry® Intelligent Security. Everywhere.