Red Balloon Security comments on: DoE RFI Ensuring the Continued Security of the United States Critical Electric Infrastructure.

Red Balloon Security
Dr. Ang Cui, CEO
David Doggett, Senior Strategist

Red Balloon Security (RBS) appreciates the opportunity to submit comments to the Department of Energy, specific to the "Development of a Long-Term Strategy" as requested in the above RFI.

Red Balloon Security is the leading U.S. company for embedded security, including analysis and exploit protection of embedded devices, and has been addressing embedded device security in a range of industries, such as telecommunications, industrial control systems, building management systems, and energy for the past 10+ years. During this time, RBS completed multiple projects for device manufacturers; performed on U.S. Government contracts for DARPA, DHS, Air Force, and other U.S. Government agencies; and internally funded research to investigate and improve the security of embedded devices, including those utilized in the electric grid.

One example of an applicable U.S. Government effort that RBS performed on was a DARPA program called Rapid Attack Detection, Isolation and Characterization Systems (RADICS) in which Red Balloon Security's embedded defense technologies were implemented into a range of embedded devices (e.g., protection relays, switches, controllers) critical for the operation and monitoring of power grids.

Red Balloon Security has the experience to provide unique insights into the security of embedded devices used in the electrical grid, including analysis of the vulnerabilities and the sources of these vulnerabilities across multiple stages of the development process and supply chain.

Response to Section A. Development of a Long-Term Strategy.

A comprehensive long-term strategy for improving and maintaining a high level of security for the U.S. electrical grid requires that equipment used in in the grid, including embedded devices must provide the appropriate level of security and significant resilience in the face of attacks. Procurement practices must both enable and enforce this level of security regardless of the source of the device.

As evidenced by RBS analysis of multiple electrical grid embedded devices and the ongoing number of vulnerabilities published on these devices by ICS-Cert, these devices are not meeting the required level of cybersecurity to counter the existing threat landscape. In addition to lacking the required level of security today, the devices are also not improving security at the rate required to keep pace with an evolving threat capability. This applies to devices sourced from within the U.S. as

well as those sourced from outside. The embedded devices being sold currently into the U.S. electrical grid are vulnerable to attack.

Sources of insecurity in embedded grid devices (e.g., RTUs, Protection Relays, Network Communication Infrastructure, etc.) include the following:

1. Insufficient security features being implemented by the manufacturer.
2. Immature implementation of secure development by the main manufacturer leading to architecture and coding gaps resulting in exploitable vulnerabilities in the devices.
3. Insufficient scrutiny on the security of components (software, firmware and hardware) used in the development of the devices leading exploitable vulnerabilities in the devices.

There is significant discussion on item 3 and how it relates to foreign ownership control or influence. The drive towards SBoM (Software Bill of Materials) as method to identify software/firmware components and potential vulnerabilities is a valuable path and should continue, but is not sufficient alone. Libraries and components developed within the U.S. supply chain often include lower level components sourced from outside the U.S. or include security issues even when developed inside the US.

Given the immature security implementation related to items 1&2—seen in both devices and components regardless of source—a minimum level of security must be set for the resulting device regardless of its supply chain origins.

Utilities have expressed a desire to purchase embedded devices with increased cybersecurity either to address current needs or to prevent the increase of cybersecurity debt in their infrastructure. Today, this is not possible as manufacturers do not have a full set of devices available that meet the level of cybersecurity desired. The cost of meeting the minimum level of security for all devices on active sale must be borne by the manufacturer as a necessary part of providing a device appropriate to its intended purpose. Any device not meeting the minimum level must only be available for sale in maintenance scenarios.

Given the growing awareness and understanding of embedded devices, the capabilities of threat actors will continue to increase, coupled with the reality that vulnerabilities will always be present in devices (even if minimized by improved procurement and manufacturing). To protect against this the devices themselves must be resilient to attacks and able to block zero-day exploits. This capability also minimizes the risk for utilities during the delay between a vulnerability becoming known, the manufacturer patching it, and the utility completing the deployment of the patch. The technology for this type of protection exists and has been deployed successfully into devices, including in the RADICS program. Due to the nature of such technologies and the high safety requirements of the electrical sector these technologies must be supported by the manufacturers on their devices vs being able to be deployed directly on devices by utilities. However manufacturers have not generally adopted technologies to enable this type of protection creating a gap in the supply chain where utilities desire the technology but the supply chain cannot provide it.

Specific Recommendations:

1. Expand the discussion to include not only supply chain sources but also to introduce a minimum level of cybersecurity for devices regardless of country of origin.

    a. Similar to how general purpose computers have antivirus, a minimum level of cybersecurity for embedded devices must include independent security technologies at the firmware level which are resilient against attacks on zero-day and other vulnerabilities (e.g., n-days) without the need to patch, thereby preventing exploitation of the devices.
    b. To enable a full understanding of attacks, devices must be enabled with the appropriate level of forensics to determine an attacker's intent once the device is accessed. This cannot be done accurately using forensics located outside of the device.
2. Address the lack of secure devices from manufacturers by engaging in ongoing security testing of currently sold devices to confirm correct implementation and ongoing ability to meet the minimum level of cybersecurity (features and robustness) in light of evolving threats. Testing must be done independently from the device manufacturer. Include publication of the list of devices meeting or failing this minimum level at the end of 1-year, banning the use of failing devices except for maintenance situations.

Implementation of the above is a core step in ensuring the long-term cybersecurity of the electrical grid, avoiding additional accumulation of cybersecurity debt on the devices that will last for years.

Red Balloon Security welcomes any opportunity to share with the DoE information on work completed and ongoing related to electrical grid embedded devices, recommended minimum security levels for devices, and exploit mitigations.