Published: April 21, 2021

Archer Brief and Opinion:

Biden's 100-day Plan to Address Cybersecurity Risks to the U.S. Electric System

On April 20, 2021, the Biden Administration announced a series of actions included in its 100-day plan to improve the cybersecurity of our nation's electric infrastructure. The plan is intended to drive significant cybersecurity improvements for the protection of "Electricity Operations from Increasing Cyber Threats". *Note: This plan does not yet appear to be available to the public at the time of publication and all comments made in this brief are based on White House and Department of Energy (DOE) snippets of what will be included in the plan.*

At the center of this effort is an expectation of direct input from electric sector industry stakeholders. In fact, the Department of Energy released an RFI to industry seeking this input. The details of this RFI can be found here - https://www.energy.gov/oe/securing-critical-electric-infrastructure

Advancing Technology

The 100-day plan states that it will **work in partnership with electric utilities and will continue to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for industrial control systems (ICS) of electric utilities**. This is an interesting push on the advancement of technology and only time will tell how this shall be achieved. Many similar attempts by the U.S. Government over the decades have generally resulted in millions of dollars being spent on solutions, without much regard for practicality or any significant reduction of cybersecurity risk.

There is a hint of "incentives" to be had when phrases such as this are used: "…encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities." Encouragement can come in many forms – financial incentives is one form, but punitive encouragement could come by way of existing compliance obligations or perhaps through licensing or relicensing processes. **One might expect that the scrutiny of the NERC CIP Standards may be ratcheted up as a by-product of this overall plan.**

Forensic capabilities is also an interesting component to be expected by an owner or operator. Cyber forensic is a serious discipline that requires explicit skills to perform properly. It would be prudent for utilities to build up their forensic plans but not necessarily their forensic capabilities. Meaning, have a specific plan in place that leads the organization in what to do and who to contact when a cyber forensic need presents itself. **Having a retainer contract or similar in place with a leading forensic firm with expertise in IT and OT would be as far as this expectation should go.**

"Enhanced detection and mitigation" tie closely with many of the NERC CIP requirements. That said, this could indicate another attempt to force industry to adopt a specific set of technologies. This has never been well received by industry, and it is to be expected that will be no different in this case. Nonetheless, **a focus on detection and mitigation highlights the need for improved security log management and overall cybersecurity risk management solutions to be implemented to a higher degree than is likely current in place for most utilities.**

The bolder statement is regarding the expectation that "over the next 100 days, owners and operators are to identify and deploy technologies and systems that enable near real time situational awareness and response capability in critical industrial control system (ICS) and operational technology (OT) networks." Not only is this extreme, but it is likely utilities cannot do more than identify and build a plan to implement within the available time allotted. **With 98 days left on the clock, purchasing the identified technology, building an implementation project, and then deploying whatever is identified leaves Archer experts scratching their head wondering who thought this was possible?** There are so many considerations with this expectation: plant outages, availability of qualified implementers (internal or external to the utility, supplier availability, how much new technology may be required.

Lastly, there is a voluntary expectation placed on the industry. That is to "deploy technologies to increase visibility of threats in ICS and OT systems." Cybersecurity volunteerism has never really worked for the electric sector. It could be different this time based on the "encouragement" to be provided to utilities but that is yet to be seen. It is also an extremely vague and potentially far too high of a bar to reach for the current level of cybersecurity maturity we have in the electric sector. This type of technology requires significant maintenance, fine-tuning and highly skilled security analysis. Then again, that is likely why it was described as a voluntary action.

Conclusion

This seems all so familiar. Back in the days when we had Richard Clarke as the United States first cybersecurity czar (1998 – 2003), there was a massive movement toward doing similar actions for the electric sector as are stated in this 100-day plan. They included town halls, government agency coordination, industry input, utility volunteerism and several requests for input from stakeholders. This has been repeated time and time again in various forms and levels of focus through efforts conducted by DOE, DHS and even as part of an Obama stimulus package component that put cybersecurity improvement at the top of the list.

Overall, this is a promising plan. It is an ambition plan. It may have some positive results, but it is likely to miss the mark in other areas. It certainly is technology heavy and seems to miss the point about "people" being half the battle. Regardless, it appears the **feds mean business and utilities will want to actively participate in the DOE stakeholder RFI** and begin taking steps to support the plan's objectives and specific expectations. This will not be easy – smaller utilities will likely find this impossible to manage without external support.

Archer has been involved with similar initiatives as utility cybersecurity program leaders, consultants, and cybersecurity government agents. With our 3 decades of experience with this type of executive cybersecurity event, we can help utilities navigate and prioritize their work efforts in a practical and efficient manner. In any event, we encourage utilities to **begin the process to plan for an expected increase in cybersecurity spend** over the next several years. This will also be the time to shore up any industry-specific cybersecurity experts, so they are readily available when the time comes to demonstrate adherence.

Lastly, this plan is likely to morph along the way. **Be sure to keep track of the Biden Administration's 100-day cybersecurity plan as closely as possible.** This will be imperative to assure expectations are being fully addressed.