THE TRANSFORMATION OF THE ENERGY SECTOR

SECURITY

DOE to vet grid's ability to reboot after a cyberattack

Blake Sobczak, E&E News reporter

Published: Friday, August 3, 2018

Department of Energy headquarters in Washington. Claudine Hellmuth/E&E News

The Department of Energy is planning an unprecedented, "hands-on" test of the grid's ability to bounce back from a blackout caused by hackers, E&E News has learned.

The "Liberty Eclipse" exercise will simulate the painstaking process of re-energizing the power grid while squaring off against a simultaneous cyberattack on electric, oil and natural gas infrastructure.

The weeklong stress test is scheduled to take place this November on **Plum Island**, a restricted site off the coast of New York that houses a Department of Homeland Security animal disease center.

DOE's goal is to "gain insights into how industry, with DOE support, would execute response to a significant cyber incident," according to planning documents obtained by E&E News.

The exercise reflects DOE's growing interest in preparing for digital threats to U.S. energy systems, an issue of "vital importance," according to Energy Secretary Rick Perry. It will also offer an early test for the new Office of Cybersecurity, Energy Security and Emergency Response, billed as a shot in the arm for DOE's handling of hacking threats.

"It's in our national security interest to continue to protect these sources of energy and to deliver them around the world," Perry said at a cybersecurity conference in New York earlier this week. "Taking care of that infrastructure, from the standpoint of protecting it from cyberattacks — I don't think it's ever been more important than it is today."

Grid-gas ties

Liberty Eclipse is expected to highlight the grid's reliance on natural gas as a fuel for power generation, a dependency that DOE officials worry could be exploited by hackers.

This summer, a leaked DOE memo proposed bailing out coal and nuclear power plants on security grounds, suggesting the nation's web of natural gas pipelines is "difficult to protect" from physical or cyber disruption (***Energywire***, June 4).

Grid security experts and some government officials have said it's hard to conclude that certain types of power generation are at greater risk for cyberattacks.

"I don't know that we've been able to make that judgment — remember that we don't have perfect visibility," Jeanette Manfra, assistant secretary for DHS's Office of Cybersecurity and Communications, told reporters earlier this week. "They're definitely a target, [but] the electric sector has a lot of resilience built into it."

Grid reliability consultant David Hilt said the huge increase in natural gas-fired power generation in recent years has introduced a "chicken and egg" problem in some parts of the U.S. in the event the lights go out.

"There are obviously some cybersecurity concerns, from both sides ... the natural gas is pumped up the pipeline by electric pumps," he said. "From an interdependency standpoint: Is everybody working together, and does everybody understand where the critical paths might be?

"I think it's good that DOE and others do these [exercises], because utilities need to get organized," Hilt said.

Testing 'blackstart'

Liberty Eclipse is set to feature a two-day tabletop exercise for grid, oil and gas executives in mid-October, ahead of the operational drill that kicks off Nov. 1. The event is not to be confused with a **2016 energy cybersecurity** exercise with the same name.

The second phase of Liberty Eclipse 2018 stands out for its focus on "blackstart" recovery, the step-by-step method for restoring electricity following massive blackouts.

Utilities can't just flip a few switches to bring the lights on following a major shutdown. In fact, power plants typically need an initial jump of electricity before they can start generating it.

Power companies rely on diesel generators and other blackstart sources to choreograph "cranking paths" for bringing the grid on its feet. Once enough pockets of electricity have been brought online, operators can sync up the islands with the wider grid.

The process can take many hours, even in the most favorable circumstances.

During Liberty Eclipse, DOE plans to incorporate simulated cranking paths provided by the Defense Advanced Research Projects Agency, which has been developing ways to speed up grid restoration following a major cyberattack. The exercise will include replicas of substation equipment so the utility industry can rehearse how it would handle a crippling cyberattack aimed at blocking participants from restoring power.

"Together, [participants] will work to energize a blackstart cranking path by detecting the attack, cleaning malicious influence, and restoring crank path digital systems to operation," the DOE states in a planning memo from last month.

Past grid cybersecurity exercises, such as the biennial GridEx event organized by the North American Electric Reliability Corp., have shied away from testing "blackstart" capabilities for fear of derailing other goals. "Doing this would limit the ability of all participants to remain fully engaged throughout the exercise," NERC has said in GridEx planning documents from past years. The grid overseer pointed out that it tests blackstart capabilities in separate exercises.

Like GridEx, Liberty Eclipse's organizers plan to put out an after-action report with lessons learned and strategies for shoring up the grid in the face of new hacking threats. The goal is to make the Liberty Eclipse series a recurring, regionally focused supplement to NERC's GridEx.

"Each iteration of the series will strive to build upon lessons learned from previous cybersecurity exercises impacting the energy sector," DOE planning documents state.

The agency's five-year plan for energy cybersecurity, prepared in March, first disclosed DOE's intention to host a new cyber-focused exercise this year. DOE said it wants to quintuple industry participation by 2019 (***Energywire***, May 15).

Time for caution

DOE has led region-specific grid security exercises in the past, in conjunction with NERC and the National Association of State Energy Officials, among others.

Alice Lippert, a former senior advisor in DOE's Office of Electricity Delivery and Energy Reliability, welcomed the revived exercise program. "It allows for better communication, so if an event does happen, they can respond more quickly and understand where the gaps are," she said.

Lippert helped direct several security exercises before leaving DOE in 2015 to work as an independent consultant.

Cybersecurity was a recurring theme, distinct from DOE efforts to prepare for hurricanes and weather-related threats.

"Cybersecurity is different: there's an unknown component," Lippert said. "Most of it is the forensics: trying to figure out where it's coming from."

A cyberattack isn't known to have ever caused a power outage in the U.S., though Russia-linked hackers have managed to reach the control system of at least one small power generator in a recent incident (***Energywire***, Aug. 1).

Lippert pointed out that utilities can come across challenges when working to restore networks found to have been infected.

"Say some system is taken down, and there's an impact. You don't know if there's some additional threat in your system before you put that all back together and get it up and running," she said. "You may be a little more cautious."