SECURITY:
DHS urged to update preparations for multiple cyberattacks

Peter Behr, E&E reporter

Published: Friday, July 8, 2016

The United States is inadequately prepared for simultaneous, large-scale cyberattacks on more than one of its critical infrastructure sectors, advisers to the Department of Homeland Security warn.

A subcommittee of the DHS Homeland Security Advisory Council has called on the Obama administration to update a 6-year-old interim National Cyber Incident Response Plan (NCIRP) with new measures to address the threat of attacks on electric utilities, telecommunications networks and the banking system all at once, compounding the damage and the restoration challenge.

"Adversaries may not do the United States the kindness of attacking only a single sector," the subcommittee **report** said, citing the cyberattack last December against three utilities in Ukraine, which blacked out power to about 225,000 customers. In addition to taking down the utilities' control systems, the attackers jammed telephone lines into the utilities, disrupting power restoration (***EnergyWire***, March 21).

"With the increasingly severity of the threat, and above all, the risk of simultaneous attacks on multiple infrastructure sectors, the need is paramount for a better integrated mechanism to coordinate across the federal government, and with the states, and with the private sector," said Paul Stockton, subcommittee co-chairman and general manager of Sonecon LLC, a security consultancy. Stockton formerly was assistant secretary of the Defense Department for homeland defense and global security.

"Our assessment is that each sector on its own is making significant progress in building preparedness to restore services after a cyberattack," Stockton added. "The challenge today is being prepared for simultaneous attacks. The attack in Ukraine gave us a taste of the threat to come."

The subcommittee criticized the interim DHS emergency response plan, saying the current NCIRP process for triggering government responses to a cyberattack based on the attack's severity was unclear and unworkable. The existing system "continues to lack the clarity needed to characterize the severity of attacks on critical infrastructure, and to set thresholds to trigger different types of response operations and the use of progressively higher levels of government authority," the report said.

DHS declined to discuss the subcommittee report or the status of the NCIRP.

"There's too much ambiguity in those [alert] categories, and it's too difficult to tell when a

particular threshold has been crossed calling for government and industry action. So we proposed a new cyber risk alert level system that is much more clear and provides a stronger base for collateral action," Stockton said.

The Obama administration is preparing to issue a new policy statement clarifying the roles of DHS, the FBI, and other federal departments and agencies in the aftermath of a major cyberattack, the report authors said, based on information from DHS. An administration spokesman declined to comment.

In a model recommended by the subcommittee, a cyberattack at the lowest level could be handled by utilities and their vendors under current legal authorities. At the fifth, or top level, of severity, a presidential declaration of emergency authorizing extraordinary responses could be necessary.

A new response plan should "jettison any reliance" on the existing system "and adopt a more operational useful way of characterizing threats," the subcommittee said.

The subcommittee also urged that governors be engaged more directly and effectively in recovery actions following a major cyberattack.

Work in progress

Issues with the NCIRP threat rating system were exposed in a DHS cybersecurity exercise in 2011 called Cyber Storm III but have not yet been addressed, according to the subcommittee.

The interim NCIRP **report** was drafted in 2008, sent to the White House the following year and published in 2010. It has remained incomplete since then, said Robert Dix Jr., policy vice president for Juniper Networks. Dix, a former staff director of the House Oversight and Government Reform Subcommittee on Information Technology, was part of the group drafting the plan.

"It is unclear who is in charge or has the responsibility for leading efforts to mitigate, respond to and recover from a cyber event that may include significant damage or disruption to data, networks, systems and critical infrastructure such as power, transportation, water, communications, information technology and more -- or even injury or death," he said.

"It is not even clear when or at what level of escalation a cyber event falls within the jurisdiction of the Department of Homeland Security or when it might have sufficient national security implications to fall under the purview of the Department of Defense," Dix wrote in a blog commentary this year.

"We have never experienced a cyber event that would qualify as a national impact [event],"

Dix added in an interview. "If we have something that begins to escalate beyond one location, one company, how do the various elements of the government react. And where does the private sector plug into the process, as the owners of the networks we rely on?

"What happens in the event of an attack we determined came from outside the continental U.S., which presents a threat not just to the homeland, but to national security?" Dix said. "Where does a transfer of authority occur from DHS to DOD?

"This has been raised in exercise after exercise for years. There was almost a fistfight right in a control center over who was in charge based on certain level of escalation in a cyberattack," he said.

Call for cross-examination

Last August, DHS Secretary Jeh Johnson asked the department's advisory group of military, law enforcement, security and academic leaders to examine cross-sector threats as DHS prepared to complete the national cyber response plan.

"We focused on the power grid, the financial services sector and the communications sector in order to bound the problem sufficiently to put out our report on time," Stockton said. The subcommittee hopes to add recommendations on water supply and other critical sectors, he said.

"We need to recognize that cyberattacks will create very different response challenges than do hurricanes and other traditional national hazards," Stockton added. Responders knew where Superstorm Sandy was going and its impact once it hit. Cyberattacks are potentially nationwide in scope, and there is no guarantee when the threats have passed, if hidden malware remains after the initial attack, he said.

"With advanced persistent cyberthreats, the risk will exist unless you scrub all the malware from your networks, that malware is going to attack again and again and again, leading to great uncertainty over restoration times and potentially severe political challenges in communicating with the American people about what they should expect," Stockton said. Sowing confusion and battering public morale may be a primary goal of attackers, he added.

The report said the relationships between federal agencies and state governors and their administrations must be clarified and strengthened. "Our focus was assuring governors have a seat at the table that's appropriate given their leading role in protecting the public health and safety of their citizens regardless of the source of the event, regardless whether it is an ice storm, hurricane or a cyberattack," Stockton said.