Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# DHS Hub To Offer Cybersecurity Boost, But Cos. Still Exposed

By **Allison Grande**

*Law360 (August 3, 2018, 10:01 PM EDT)* -- The U.S. Department of Homeland Security's recent decision to open a center dedicated to tackling cyberthreats directed at critical infrastructure is likely to help expand vital communication channels between the public and private sectors, but lingering concerns over liability protections could limit the initiative's ultimate effectiveness, attorneys say.

The new National Risk Management Center, which was announced during a cybersecurity summit hosted by the Trump administration in New York City on Tuesday, will be tasked with coordinating national efforts to protect U.S. banks, electric companies, telecoms and other critical infrastructure operators from increasingly prevalent threats from nation states such as Russia and Iran.

While several efforts have been launched in recent years to bolster sharing of security threat information between the federal government and private companies, the new center's focus on working across industry lines to develop risk management strategies could significantly improve how these threats are identified and addressed, according to attorneys. However, details on how exactly the center will engage with and protect critical infrastructure operators from exposure are sparse, leading some onlookers to remain skeptical that the initiative will drastically move the needle on security preparedness.

"To the extent that DHS is trying to use this center to foster conversation and stay ahead of the curve on cyberthreats to critical infrastructure, that's great," said Davis Wright Tremaine LLP partner Christopher Ott, a former senior counterintelligence and cyber counsel with the U.S. Department of Justice's National Security Division. "But its ultimate success is going to hinge on years of hard work and engagement, not in what they have announced thus far."

In order to be effective, the center will need to gather threat information and share it with relevant public and private sector stakeholders in a timely manner, Ott noted. These efforts necessarily raise questions over how to sanitize information in a way that still renders it useful and how to ensure companies don't face unforeseen consequences as a result of their participation, difficulties that have to date stunted the spread of existing initiatives such as the Homeland Security Information Network and the National Cybersecurity and Communications Integration Center, according to Ott.

"If those challenges are not substantively addressed by this new center, it is unclear what additional help DHS is providing," Ott said.

In a speech at the recent cybersecurity summit, Homeland Security Secretary Kirstjen Nielsen noted that the new center is intended to break down "silos" that have resulted in stakeholders focusing too closely on one event rather than taking a bigger picture look at threats and failing to coordinate plans with those outside their industry.

According to Nielsen, the center is intended to go beyond previous efforts such as the National Cybersecurity and Communications Integration Center, or NCCIC, which opened in 2009 as a hub where DHS could monitor threats across critical infrastructure but shifted its focus to working more collaboratively on these issues with the private sector as a result of the passage of the Cyber Information Sharing Act in December 2015.

The NCCIC will continue to remain DHS' central hub for information security operations focused on real-time threat indicator sharing and incident response, while the new center will focus on understanding what threats are truly critical to these companies, and how stakeholders can communicate more efficiently to reduce strategic risk.

This breakdown of responsibilities is likely to prove beneficial to critical infrastructure companies that choose to participate in the new center by helping to ease the difficult work of connecting with those in other sectors and maintaining those relationships, according to attorneys.

"Everyone understands that the compromise of critical infrastructure networks can lead to major repercussions across sectors, so an emphasis on risk management and thinking through these issues with a very wide lens could be useful in helping companies in different sectors learn from those that may have more experience dealing with these threats and working with the government," said Mayer Brown LLP partner Stephen Lilley.

Nielsen repeatedly stressed in her speech that neither the public nor private sector can tackle these threats on their own, given that companies generally have a grasp of what's happening in their systems and the government tends to have separate intelligence about the origin of the attack. The rapidly growing pace and severity of such attacks, which include efforts by Russian-backed actors to interfere with and influence U.S. elections and hackers with ties to North Korea and China breaking into systems at Sony and the Office of Personnel Management, also demand more coordinated action, the secretary said.

By bringing these sides closer together and providing companies with a single point of access through the center, DHS is at the very least laying the groundwork for a model that makes more sense in an age where increased connectivity is providing more points of access for bad actors, attorneys say.

"From a cybersecurity perspective, it makes a lot of sense to be holding exercises to contemplate how vulnerabilities in a shared products could impact different kind of sectors," Lilley said. "There's been a tendency in data security of creating silos, and this seems like a natural progression in efforts to build relationships across sectors."

With the creation of the center, the NCCIC will be freed to focus on the day-to-day work of helping the public sector and infrastructure operators respond to threats — the function it was designed for — while more attention than ever can be devoted to the longer-term strategic planning and analysis necessary to combat threats to critical infrastructure.

"The government's solution is almost always to create more bureaucracy, which is often misguided, but

in this context it makes sense to divide out the mission of NCCIC when it comes to big-picture strategic planning," said Seth Stodder, a Holland & Knight LLP partner who served in various roles with DHS during the Obama and George W. Bush administrations.

The approach is similar to that employed by the Office of the Director of National Intelligence, which has separate arms that deal with day-to-day operational intelligence functions and with bigger-picture intelligence analysis and strategic planning, Stodder noted. But the division between real-time threat monitoring and long-term risk management, as well as the center's planned emphasis on pushing companies to share information outside their sector, has yet to be tested in the information security space.

"This new emphasis on risk management and cross-sector approaches is something that hasn't necessarily been emphasized by DHS yet in its outreach to businesses," Lilley said. "DHS seems to be making the judgment that this reorganization and reprioritization will help advance the issues, and if industry partners support the effort and are able to provide DHS with support, the agency may be proven right."

However, how broadly industry buys in will be remains to be seen.

During the summit, some major private industry stakeholders — most notably AT&T Communications CEO John Donovan — repeatedly stressed the importance of sharing information on increasingly prevalent threats and risks confronting infrastructure operators, and attorneys say the enthusiastic involvement of these type of entities could pave the way for broader private industry participation.

"Having very vocal leaders at the summit talking about how a center like this was overdue and the government needed to step up in this area, that's a hopeful sign," Stodder said.

He pointed out that the Customs-Trade Partnership Against Terrorism, a voluntary supply-chain security program led by U.S. Customs and Border Protection, was initially stood up in 2001 with the participation of only seven large U.S. companies, including Walmart, Target, Ford, Motorola and Sara Lee. The program now has more than 10,000 certified partners.

Megan Brown, a Wiley Rein LLP partner and former senior DOJ official in the George W. Bush administration, noted that even just a few years ago "it was hard for companies to justify caring about and investigating in cybersecurity." But the current threat landscape — with attacks ranging from the breach of the electric system in Ukraine in 2015 to the seizure last year of health care systems and other infrastructure worldwide through the WannaCry virus — has helped to make companies more comfortable with working together and with the government to share threat information, Brown said.

But attorneys were quick to note that DHS has said that while businesses seem interested in receiving threat intelligence from the government, only a handful of companies have signed up to share information about what they're seeing with the government through the NCCIC. Much of this hesitance comes from concerns over what the government may do with this information and whether other regulators or competitors will be able to access it and use it against them.

While companies were given some liability protections in the 2015 Cyber Information Sharing Act, Trump administration officials in revealing the new risk management center didn't discuss how companies who participate in discussions and risk management planning will be shielded from legal exposure, leading to predictions that the center may face the same fate as previous efforts.

"Generally speaking, the same type of legal risks that have existed with engaging with DHS in the past are going to continue," Lilley said, adding that those companies that have already gone through the process of thinking through liability issues that could be raised by this sharing and establishing are "going to be in a better position to engage with the government, and are the ones that will be most likely to participate in the center and maybe pull companies that are not as mature into the fold."

The center may additionally introduce fresh legal concerns if it proves to be inconsistent with steps taken by other federal agencies, such as the U.S. Department of Defense, according to attorneys.

"While DOD does not have any jurisdiction over DHS, I think it is important that these agencies coordinate their efforts for several reasons," said Robert Huffman, leader of Akin Gump Strauss Hauer & Feld LLP's government contracts practice. "One reason is that many government contractors contract with both agencies and it will be difficult to comply with two different and potentially diverging requirements."

Even if most companies don't show an interest in the newest DHS information-sharing and risk management effort right away, attorneys say the move to launch the center proves that the Trump administration is highly concerned about the threat posed to critical infrastructure and that it favors closer collaboration with the private sector to tackle these efforts.

In her speech at the summit, Nielsen said that a "Cat 5 hurricane has been forecast" and that the U.S. was "in crisis mode" when it came to information security. She stressed that "cyber threats collectively now exceed the danger of physical attacks against us," and that "if we prepare individually, we will surely fail collectively."

She urged the convened stakeholders, who included more than 20 CEOs from some of the world's largest companies and other senior government officials, to work together with "clear-eyed urgency" in order to "turn the tide" in order to "repel digital invaders" and safeguard critical networks.

"The tone in the speeches at the cybersecurity summit seemed to be more urgent and alarmed than we've heard the government be on cybersecurity before," said Brown, who participated in a panel at the summit. "It seems as though they're seeing things that they're worried about and want to accelerate the good work that's already going on in the private sector, and this is an effort to put that on steroids a little bit."

Vice President Mike Pence also delivered his first-ever remarks on information security at the summit, touting his colleagues' work on handling the "cyber crisis" he said they inherited from the Obama administration, which he claimed "let the American people down when it came to cyber defense" and "all but neglected cybersecurity."

But several attorneys said after the summit that the center struck them as being the next logical step in building on efforts by previous administrations to tackle these threats.

"The Trump administration's approach on cybersecurity seems to be pretty consistent with the Obama administration," Stodder said. "It's been an evolution more than an revolution from Obama to Trump in this area."

With no end in sight for these efforts, attorneys added that while much of the focus is on critical

infrastructure at the moment, any effort to shore up security in this area is likely to have a trickle-down effect to less vital sectors such as retail and hospitality, given the cascading effect an attack on the electric grid or financial system could have on the entire corporate ecosystem.

Brown pointed out a voluntary security framework developed specifically for critical infrastructure operators by the National Institute of Standards and Technology in 2014 has ended up being adopted by a wide range of noncritical businesses, and attorneys predicted that any standards drawn or lessons learned from the work done at the new DHS risk management center could be applied far more broadly than just critical infrastructure.

"Everyone depends on critical infrastructure in one way or another, so if these efforts are effective and responses to incidents and protections surrounding critical infrastructure become more effective, that would be a rising sea that raises all boats," Lilley said.

--Editing by Brian Baresch and Jill Coffey.

---