DHS’ Newly Launched Risk Management Center to Boost Information Sharing

“We must move beyond routine information sharing,” said Secretary Kirstjen Nielsen.

NEW YORK CITY — The Homeland Security Department this week opened the doors to a cross-sector central hub for government experts and industry partners to more effectively share information, tailor cyberassessments and defend the nation’s critical infrastructure.

“For far, far too long, we’ve lacked a single focal point to bring government and industry together to assess the digital dangers we face and to counter them,” said DHS Secretary Kirstjen Nielsen in announcing the new center July 31 at the DHS Cybersecurity Summit in New York City.

Photo: Amanda Ziadeh/GovernmentCIO Media

DHS Secretary Kirstjen Nielsen at the DHS Cybersecurity Summit in New York City.
Summit. “A place where analysts and network defenders can address these risks together.”

The National Risk Management Center will be housed at DHS and is driven by the needs of industry, meaning private sector partners will influence how DHS supports them, Nielsen explained. The goal is to simplify the process of reporting and identifying threats, and to create a single point of access to the full range of government cyberthreat activities.

So, rather than calling 911 when a state or local entity, or even a company, is under a cyberattack (which apparently does happen), Nielsen said “the best thing to do will be to call this center.”

But why a center entirely focused on risk management?

The need for this model is brought by the reemergence of the nation-state threat, a hyperconnected digital environment and the desire to effectively and continuously work with industry.

Nielsen said the center will also be taking pieces of threat intelligence and work with private sector partners to answer the “so what” of the threat, and, basically, what to do about it.

Think of cyberthreat data like a puzzle piece: The private sector will help DHS identify where that piece fits in, the trends and threads it is associated with, the purpose of the attack and the implications.

“This is where the expertise of the private sector comes in, to help us contextualize the threat,” Nielsen said, throughout the planning, mitigation, response and recovery phases. DHS is well aware the private sector knows its operational environment best, so it needs industry expertise to understand how these pieces fit together.

DHS isn’t wasting any time, either. Nielsen said the center will begin with a trisector approach focusing on the financial services, telecommunications and energy sectors, and will drive forward with 90-day sprint models starting immediately. These sprints are meant to identify those key priority areas, conduct joint risk assessments and eventually, lead to a cross-sector cybersecurity exercise this fall.
This way, DHS can tailor its assessments, plans and playbooks to the proper sectors.

“We will look to you to influence how we can support you best,” Nielsen said.

This announcement comes on the heels of recent DHS cybersecurity talks related to election security, critical infrastructure and national security. Building a collective defense and bolstering information sharing between government and private partners isn’t a new concept by any means, but the center intends to make it easier to work cross-sector, engage daily and then respond appropriately.

And the center is just one of the efforts underway. Nielsen said DHS is also reorganizing itself and working with Congress to pass legislation on a new Cybersecurity and Infrastructure Security Agency within DHS. This agency would recast DHS’ current cybersecurity arm, the National Protection and Programs Directorate, into an operational agency better equipped to confront threats.

In the meantime while DHS awaits approval for the new agency, the National Risk Management Center plans to help the nation stay ahead of cyberadversaries.