Homeland Security Restructures to Face Evolving Cybersecurity Landscape

First the National Risk Management Center, now the Cybersecurity and Infrastructure Security Agency.

Amanda Ziadeh

Wed, 10/10/2018 - 09:10

DHS Undersecretary Christopher Krebs at GovernmentCIO Media's CXO Tech Forum: The State of Cyber Oct. 4. (Geoff Livingston/GovernmentCIO Media)

The Homeland Security Department's National Protection and Programs Directorate was founded in 2007 under a different national threat landscape, and a new title could better represent the cyberthreats and critical infrastructure risks faced today.

A name may seem like just a name, but it's much more to NPPD. "It clarifies and signifies our mission," said DHS Undersecretary Christopher Krebs, in a fireside chat Oct. 4 at GovernmentCIO Media's CXO Tech Forum: The State of Cyber.

On Oct. 3, the Senate passed the Cybersecurity and Infrastructure Security Agency Act, which will rebrand DHS' NPPD to the Cybersecurity and Infrastructure Security Agency, and put Krebs as the agency's director. The legislation is on its way to the President's desk.

Aside from no longer having to explain what the NPPD means to the private sector and critical infrastructure community, Krebs said the name change will help with recruiting, and most importantly, streamline the organization.

"When [NPPD] was established in 2007, it was almost like an island of misfit toys," Krebs said, as it held disparate security programs within DHS that didn't seem to fit under other established legacy agencies. There was the Office of Cybersecurity and Communications, the Office of Biometric Identity Management, the Federal Protective Service, and a suite of programs that mission-wise, didn't directly align.

So, as the cyberthreat landscape evolved over the years and the department's role strengthened by Congress, Krebs said it became clear that the department needed "a single voice, a single agency or organization able to carry out the secretary's critical infrastructure protection and cybersecurity authorities."

This means that some of those programs currently within NPPD will be reassigned under other offices to better position CISA, and there will be a transition process before getting fully operational. "These are critically important missions for the department and the broader security enterprise, but they're not core to the mission of CISA," Krebs said.

But this name change is a critical moment for the organization in order for it to properly reorganize and refocus.

An Awakening

When the intelligence community got wind of how the Russian intelligence agencies were attempting, and in some cases, infiltrating, state election infrastructure in 2016, and when DHS received that intelligence, Krebs said it took "a while" to figure

out who to talk to.

“The concept that secretaries of states administered elections was not something that DHS or the intelligence community knew,” he said. The agency that did have a deep understanding of this is the Election Assistance Commission. The problem was, “no one in DHS knew that the Election Assistance Commission actually existed,” so a digital exchange of business cards was happening during incident response.

DHS has gotten past this, it understands the landscape and the players, and partnership mechanisms and communication protocols have since been established, Krebs said.

“Now, I have a piece of intelligence, actionable intelligence, I know who to go to in every single state,” Krebs said. NPPD created the Election Infrastructure Information Sharing and Analysis Center in February. It has nearly 1,000 members and is comprised of all 50 states and local jurisdictions.

But Russia’s efforts to interfere with the 2016 elections was an awakening for the IC and American public, because it showed just how impactful cybersecurity can be, and how it could destabilize the government. As a result, Krebs said he’s seen all those involved — the IC, the FBI, the State Department, etc. — orient towards a single goal, and work to align capabilities and resources towards a common adversary in ways that support the federal, state and local governments.

“Every one of the missions within DHS serves a critical purpose. What we need to do 15 years into the department is ensure that we’re properly aligned across the mission space to achieve those security outcomes we want, and that’s the primary objective of the CISA legislation,” Krebs said.

Reorganizing for Private Sector Involvement

This isn’t the agency’s first restructuring this year, either. DHS Secretary Kirstjen Nielsen announced a new National Risk Management Center July 31, which will take threat intelligence and work with the private sector to decide what to do with that threat. The center is taking a trisector approach, focusing on the financial services, telecommunications and energy sectors.

“What this was . . . was taking an existing organization or subcomponent with NPPD,

my team, that was kind of a back office risk analytic shop that took some good demand signal and generated good analytic product," Krebs said, but it was lacking a strong connection with the private sector.

So, the center is more private sector informed, which Krebs said is consistent with a broader philosophy he's bringing to the organizanization. "We're not doing anything, for the most part, without having a clear set of requirements established by the private sector and our critical infrastructure partners."

View printer friendly version
Department of Homeland Security
cyber
Federal Cybersecurity
Christopher Krebs
National Risk Management Center
CXO Tech Forum State Cyber