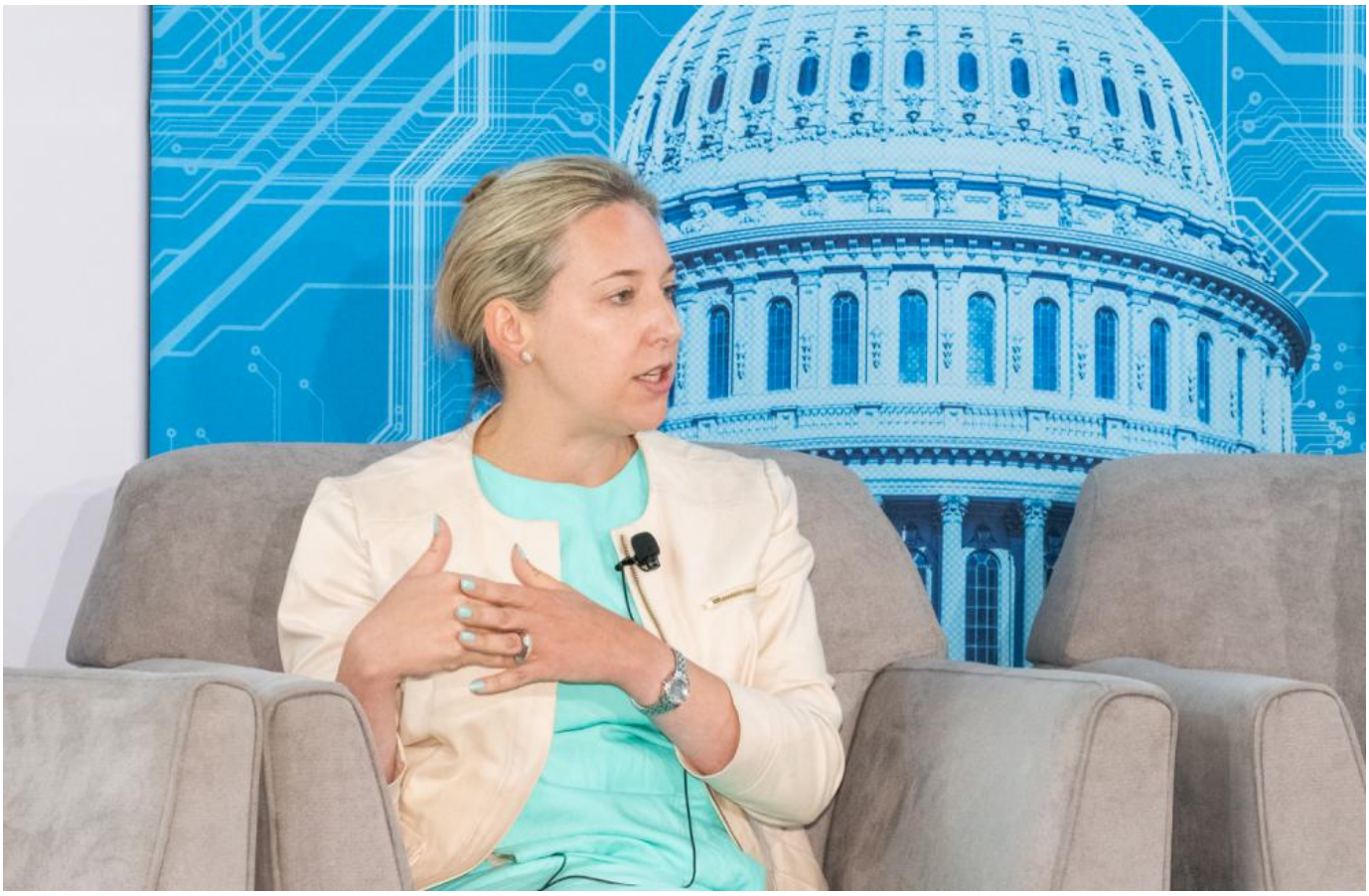
CISA: Managing Security Threats Requires Collaboration From Government, Industry

Assistant Director for Cybersecurity Jeanette Manfra talks through the newest agency's focus areas and mission.

Amy Kluber

Fri, 07/19/2019 - 17:26



Assistant Director for Cybersecurity at DHS' Cybersecurity and Security Infrastructure Agency Jeanette Manfra talks through the agency's goals at State of Cyber CXO Tech Forum. Photo Credit: Geoff Livingston

Tackling some of our nation’s most difficult and complex security threats requires a well-rounded and collaborative approach, according to one Department of Homeland Security leading official at this week’s State of Cyber CXO Tech Forum.

The agency’s newest unit, the Cybersecurity and Infrastructure Security Agency, was recently stood up by Congress in November 2018 to improve cybersecurity across government. And according to Assistant Director for Cybersecurity Jeanette Manfra, CISA sees collaboration with government and industry and managing enterprise risk to be key toward a resilient and secure future.

“It has to be a conversation between the security people, the engineers and the mission people,” said Manfra during a fireside chat at the event. “It can’t be security people trying to make decisions on one side, engineers developing the system on another side and the mission people on the other side.”

This notion forms the backbone of the agency, whose inherent mission is to partner with the public and private sectors to understand and manage risk to our critical infrastructure.

Manfra stressed the importance the agency plays in overall government. Some of its early beginnings stemmed back to DHS’ National Protection and Programs Directorate created as part of the post-9/11 response.

“The key part was there was no clear mechanisms or clear authorities on who and how the government would partner with critical infrastructure,” said Manfra. “How do we partner with some entities that have some threat on the prevention side to raise the bar on security … but also to build resilience?”

As part of this role, CISA has authority to issue binding directives to set requirements for federal agencies in cybersecurity areas, Manfra explained.

“We thought about how to issue these and we wanted to focus on something representative of an enterprise risk, not just focusing on a couple agencies,” she explained. “We found the authority is very useful in driving better practices beyond the federal government … taking the federal government from being as sort of the laggards in industry on certain security practices to actually leading.”

Addressing critical infrastructure is another gap the agency fills through its National Risk Management Center, which aims to identify and address significant risks to critical infrastructure through collaborative efforts with the private sector, government and other stakeholders. In April, the center released its first set of national critical functions that are “so vital to the U.S. that their disruption, corruption or dysfunction would have a debilitating effect on security, national economic security, national public health or safety,” according to CISA.

“This was the first step … looking across the country saying, ‘What are we most concerned about being disrupted?’” Manfra said.

When it comes to technology modernization, Manfra stressed the importance of looking at it from a broader perspective to incorporate not just the physical technology, but also other elements such as policy, acquisition and supply chain.

“There’s a lot more to modernization,” she said. “It’s certainly not the CISOs that doesn’t think in a risk-based approach, it’s more so the auditors, it’s the folks doing the ATOs … How do we get everybody to think about these high-value assets, how do we prioritize resources, how do we take actions to make ourselves overall more secure, and how do we become more flexible and resilient as a government?”

As for the policy side of security, new or changing policies is not always the answer. Manfra stressed there are still some things CISA is looking to figuring out how to best apply this collaborative way of thinking when it comes to policy.

“There are no conclusions about what is needed,” she said. “We don’t want to make conclusions until we go through a more deliberate process of understanding what would be the benefit of changing any regime that we have right now."

View printer friendly version
CXO Tech Forum State Cyber 2019
cyberattacks
Federal Cybersecurity
National Risk Management Center
risk management
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Standard