How DHS Executives Weather the Pandemic and Concurring IT Challenges

Automation, Agile and DevOps could be the blueprints for IT modernization.

Kate Macri
Wed, 11/25/2020 - 08:04

Accommodating the mass shift to telework at the beginning of the COVID-19 pandemic is just one challenge DHS executives faced this year. Executives also realized they needed to accelerate their IT modernization and security strategies to create a more agile department ready for abrupt change.

Brian Burns, deputy CIO for the Coast Guard, said he sees DevSecOps, artificial intelligence and automation as key drivers of IT modernization for the service.
“We see DevSecOps as a critical component for moving us into a modernized environment,” he said at a November DHS Industry Day conference. “Our first project is our vessel documentation system. If you have a car, you go to your local [Department of Motor Vehicles] and register your car. [Our system] is for registering U.S. flag vessels, and it's going to improve our governance processes [and help us get] to continuous integration and delivery as we move forward.”

The Coast Guard wants to automate its ATO process to constantly validate cloud infrastructure to prevent any hiccups or delays in IT operations and delivery, he added. The Coast Guard recently established a Data Readiness Task Force, he added, to help progress the Coast Guard’s AI strategy

“AI is going to be the future in terms of ...[our ability] to explain data,” Burns said.

The Coast Guard isn’t the only DHS component exploring AI. Russell Roberts, CIO of the Transportation Security Administration (TSA), wants to use AI and machine learning to detect threats in airports, but said these technologies will require 5G bandwidth.

“We're looking for industry to help partner with us on this,” he said at the conference.

TSA also looks to DevOps and Agile practices to ramp up its IT modernization efforts.

“We're very Agile. My staff is very good at it. We continue to move in that direction,” Roberts said.

One area Roberts looks to industry for assistance is cybersecurity, which is one of his biggest concerns given the TSA’s budget constraints.

“We're all under extreme pressure with our expertise in the cyber world. What's keeping me up at night ... not having the professionals to do something when something goes wrong,” he said. “[We want to] automate everything. The way we do ATOs, those are challenges for us because the mission requests never slow down. The number of people are pretty finite and my budget continues to shrink.”
Karen Evans, CIO for all of DHS, said she dramatically accelerated CIO mission priorities to consolidate data centers and security centers and move from legacy IT systems to the cloud when she took office in June this year.

“The CIO team ramped up the telework communications, we had about 5,000 people on concurrent telework on the VPN, now on an average day we have 55,000 concurrent on the VPN,” she said. “I don't think we missed anything, what we've really done is shifted the way we do work and accelerated different implementations and also shifted the security associated with the remote workforce to reduce the risk.”

Richard McComb, DHS' chief security officer, said the department follows OMB guidelines with regard to security in a remote work environment, and allowed for flexibility when onboarding new DHS employees.

For example, instead of requiring physical fingerprinting for new employees, DHS used virtual identity proofing, he said.

As various DHS components continue to ramp up IT modernization efforts and bend and shift to adapt to the coronavirus pandemic’s influence on work, DHS headquarters leans on industry partners to accomplish its mission objectives.

“Industry can help DHS by DHS being a better customer,” said DHS Chief Readiness Support Officer Tom Chaleki. “If DHS could establish better requirements, consistent requirements, clear long-term objectives and understand some of the pressures the industry is under — I think we have a much better partnership.”
agile
automation
ATO
Standard