PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

MICHELE THOMAS

CISO
United States Department of Agriculture - Animal and Plant Health Inspection Agency

Headquarters: Riverdale, MD
Agency Size: 8,000-10,000

SMART AND EFFECTIVE REGULATORY RESPONSE DRIVES SECURITY AT THE USDA

Michele Thomas is the CISO for the Animal and Plant Health Inspection Service (APHIS) agency of the USDA. The USDA is the second largest civilian government agency in the United States and APHIS is one of its largest component agencies, with between 8,000 and 10,000 employees. Thomas' responsibilities include risk, compliance, identity management policy and guidance, and cybersecurity operations.

As one might expect, being CISO at a major government agency, most of Thomas' time and attention is spent ensuring that the organization is meeting cybersecurity regulations. For example, according to FISMA regulations, a system must be reaccredited every three years. This means that Thomas' staff must review systems against hundreds of controls and then submit a report to the Security Control Assessor, a high-ranking official outside of the risk and compliance team. The CIO fulfills that role at APHIS. The Security Control Assessor then submits a request to the Approving Authority to approve the system for production use. While some balk at this level of reporting and auditing, Thomas believes that it is vital to ensuring security controls are met that enhance an organization's cybersecurity posture. If the private sector set policies to mandate these types of checks to the degree the government has, Thomas believes that certain news-making breaches would have been prevented, or in the least, had a smaller impact.

ADAPTING TO CHANGE: NEW CYBERSECURITY BILLS MEAN A CHANGE IN PROCESS

Change is hard for anyone, whether in the public or private sector. In December of 2014, the President of the United States signed

several cybersecurity bills into law. As a result, the government essentially redefined how it handled, managed, and administered cybersecurity across the government. Congress legislated that the Department of Homeland Security (DHS) would manage cybersecurity for all federal agencies. This program institutionalizes Continuous Diagnostics and Mitigation (CDM), meaning each agency must continuously monitor their networks and cyber incidents, and report results every 72 hours to DHS. The regulations are recent enough that the USDA has just kicked off its program. As a result Thomas' main challenge for this year is digesting the new requirements and implementing appropriate USDA processes and solutions to meet these requirements. She says, "I'm not worried about it, but it will be a challenge when the fire hose turns on and we have to implement the appropriate changes."

One thing that will not be a challenge for Thomas is budget - at least in this instance. Congress has allocated spending for the CDM project, so it will not affect her overall security budget, which otherwise has seen cuts, just like every other federal agency.

WORKING SMARTLY WITHIN REGULATIONS

Because much of what the USDA does is regulated, Thomas believes that at times, the Agency automatically defaults to unnecessarily strict interpretations of the guidelines. Her job is to help USDA APHIS employees understand how to work efficiently within the standards. For example, there are regulations within the USDA mandating that every mobile device with access to IT systems must be connected to mobile device management software. Recently, an emergency operation involved sending staffers on location with iPads to map a pest infestation. When the group came to Michele's team for device management software, she explained to them that it was not required because they would not be accessing USDA systems from their iPads. The distinction meant the team was able to begin mapping the infestation much more quickly, and at a lower overall cost to the agency.

Advice for Private Sector CISOs: Know What You Don't Know

For many years, Thomas has worked in the US government, but she previously had a career in the financial services industry. She believes the government is more advanced than the private sector when it comes to prioritizing cybersecurity and creating strong cybersecurity programs. She credits much of this to regulations, which she acknowledges may be a dirty word to some in the private sector. However, she says that between the government's focus on cybersecurity, specifically the recent Cybersecurity bills passed by the White House, the government is more forward-thinking than the private industry, when it comes to response and planning. "In my personal opinion, it doesn't take Target, Sony, or Anthem to show that the private sector lacks a sense of urgency. Our urgency in government agencies on the other hand, has been mandated by law. However, the current situation with the OPM breach illustrates that just having standards, policies, and regulations is insufficient. One must actually follow and implement them! That's exactly what DHS hopes to do with the CDM Program."

Thomas offers the following advice to her private sector peers: "Get the best consultants and experts you can find, and have them tell you what you don't already know. Take a look at your biggest vulnerabilities –make sure you know the hardware and software on your network and the operating systems they run. Make sure you know how you will manage those vulnerabilities and the processes you can put in place to mitigate them. Make sure you have an emergency response plan in place. Many companies do, but just as many do not." And to her government peers, she says "Implement!"