DoD unveils new cybersecurity certification model for contractors

By Nicole Ogrysko | @nogryskoWFED

The Defense Department sees its new certification model, which it unveiled to the public this week, as a way to more quickly bring its entire industrial base up to date with best cybersecurity practices.

But the Pentagon also sees this new model as a means to set the stage for a broader, more complex journey to better understand the defense supply chain.

On Wednesday, DoD released a new draft of the Cybersecurity Maturity Model Certification (CMMC), the Pentagon's most recent to attempt to create a simpler, more consistent framework for the cyber demands it imposes on its contractors and subcontractors.

The department will accept public comment on the certification model through Sept. 25.

"Every company within the DoD supply chain — not just the defense industrial base, but the 300,000 contractors — are going to have to get certified to do work with the Department of Defense," Katie Arrington, chief information security officer for DoD's Office of the Assistant Secretary of Defense for Acquisition, said Wednesday at the Intelligence and National Security Summit co-hosted by AFCEA and the Intelligence and National Security Alliance.

Certification model details five levels

The new certification model has been designed with several familiar cybersecurity requirements in mind, but it's also an attempt to get a better handle on the defense supply chain, Arrington said.

The model covers 18 domains based on five levels.

Companies who achieve certification at the third level, for example, meet all National Institute of Standards and Technology (NIST) SP 800-171 requirements and have an information security continuity plan. Firms assessed at level five have "highly advanced cybersecurity practices" and can respond at "machine speed," according to the draft CMMC.

DoD, which has been developing the certification model since March, has partnered with Johns Hopkins University, Carnegie Mellon University, defense industrial associations and members of the Defense Industrial Base Sector Coordinating Council to design the program.

DoD will release the model to a consortium in January 2020, which will help contractors learn the CMMC and the steps necessary to achieve each level of the certification program.

The model will go live and will begin to appear in requests for information next June and requests for proposal later that fall, Arrington said.

Every Defense contract will use this scale to determine whether companies are allowed to bid.

“We understand security will be an allowable cost,” Arrington said. “We know what we’re asking for, but if we value security as delivered uncompromised, stated very clearly, the cost, schedule and performance don’t function without security. They’re invaluable.”

Arrington, along with the Department of Homeland Security and members of the Federal Acquisition Supply Chain Council, are reviewing cybersecurity standards and using DoD’s new model as a starting point for broader conversations about the defense supply chain.

“We get everyone on a level-set playing field for cybersecurity, and then we can really start looking at our supply chain, where our most and greatest vulnerabilities lie and how we can work together in a collaborative event with industry,” she said. “With 70%-plus of our data living on your networks, it is no longer a moment. It’s [not] a me-thing or a you-thing; it’s a we-thing.”

But for large defense contractors like Lockheed Martin, the new cybersecurity certification program could, at least initially, look like DoD is piling on yet another series of standards on top of an already growing list of NIST requirements.

Too many scoring methodologies and cybersecurity assessments from individual services and Defense agencies pose too much complexity, said Scott Rush, Lockheed’s deputy chief information security officer.

“We’re seeing a lot of different requirements come across,” he said. “For a large enterprise that, from an unclassified perspective, manages a large IT environment [and] common systems to support multiple programs and contracts, having a different set of requirements becomes very problematic.”

Though Rush said building the maturity model into the acquisition process makes sense, he’s hoping to see more uniform, common cybersecurity standards across the Defense enterprise.

“To bid on a contract or perform you have be maturity level 3 or you can’t perform, we understand that and we think that’s a good thing,” he said. “What we would rather not see happen, because we think it would dampen collaboration, is if it becomes part of the evaluation criteria.”

Arrington acknowledged those concerns. She sees DoD's new cybersecurity model as a way to move past the array of disparate and scattered requirements and toward an environment that's focused on protecting the defense supply chain.

"I've met with all the services, and they have bought into the CMMC being the one cybersecurity model that they'll be using for the DoD," she said. "Hopefully we can convince our partners in the federal acquisition side to adopt it as well."

Supply chain illumination 'pathfinders' picking up steam

Meanwhile, DoD is continuing to explore ways it can realize the full scope of its supply chain.

Lockheed Martin, for example, has been working with the Missile Defense Agency (MDA) to build a tool that will identify where controlled defense information resides within each "tier" of multi-layered defense contract.

The Missile Defense Agency is reviewing the results of Lockheed's pilot, which has been ongoing for eight-to-nine months, Rush said.

"We've learned a lot in terms of how to roll something like this out in a multi-tier supply chain," Rush said. "We've learned a lot about the requirements they need and they don't need, and I think it's really going to inform a path forward from an MDA perspective. [The agency] has been talking… to [Arrington] and others in DoD about how this might apply to broader illumination efforts."

For Arrington, the supply chain dashboards that Lockheed Martin and others have been piloting show some promise. But they leave a big question unanswered.

"The challenge is: where do [you] maintain that data inside the DoD? That's a big one," Arrington said. "That's our adversaries' golden egg. It's a classified system, ultimately, but we also have the visibility within the MDA models."

Using these dashboards to identify and then share information about potential risks and vulnerabilities on the supply chain with other services and members of the defense industrial base is the next challenge.

"If we can figure out a way to mitigate that risk within the supply chain, and we can buy down the risk and buy up the uncertainty, that's what we want in these illumination tools," Arrington said. "We are moving to them. Congress has put money appropriated for them. This is happening. What we're deciding now are what are the requirements, what are we looking at and what is the value-add and the visibility?"