# CIO Council, OMB identifying the pieces to complete the zero trust puzzle

**By Jason Miller**
**May 17, 2019**

https://federalnewsnetwork.com/ask-the-cio/2019/05/cio-council-omb-identifying-the-pieces-to-complete-the-zero-trust-puzzle/

The litany of programs focused on federal cybersecurity from continuous diagnostics and mitigation (CDM) to Einstein to high-valued assets to IT modernization seem to go on forever.

But there is that proverbial light at the end of the tunnel that will bring many of these initiatives together.

Suzette Kent, the federal chief information officer, said the time is right to think about how the concept of zero trust underpins all of these efforts.


Federal CIO Suzette Kent.

"Each of those pieces is part of the puzzle. We want to have perspectives so that agencies are touching these other components, they are doing it with a long-term vision in mind," Kent said on Ask the CIO. "In conjunction with these other transitions, which really was one of the drivers, we partnered with ACT-IAC because we wanted to bring in perspectives from what was done out in the industry. Not just the technology components, but we wanted to know how you get there and what is the sequence in which you think about moving these different pieces."

ACT-IAC, at the behest of the CIO Council, wrote and released a zero trust white paper last month describing the current state of technology and the commercial market, and what are some of the emerging best practices to move toward this framework.

"Implementing zero trust does not require a wholesale replacement of existing networks or a massive acquisition of new technologies. ZT should augment other existing cybersecurity practices and tools," the white paper states. "Many federal agencies already have elements of ZT in their infrastructure and follow practices that support it in their day-to-day operations. Elements such as identity credential and access management (ICAM), access standards based on trust algorithms, automated policy decisions, and continuous monitoring are critical complements to a successful ZT."

Kent said despite all the buzz and excitement around zero trust, the end goal remains the same for agencies—modernization.

She said zero trust just happens to be a modern framework for organizations to know who is on the network and what they can get to in terms of data and systems.

"It's a critical framework for us to be able to have to protect that data and operate in the environment," she said. "This is a critical technique and that's what we heard from the council is that it's a set of techniques that they wanted to understand more while they were touching the various moving parts and making sure they were designing with this in mind where appropriate."

## TIC policy uses cases

Steven Hernandez, the chief information security officer at the Education Department and a member of the white paper's project leadership team, said ACT-IAC initially began looking at zero trust networks and software-defined networks, but soon realized this concept is much bigger and touches the entire technology layer.

"The big takeaways for us from an operations and strategy perspective, in the government space we have to understand the mission. Are we talking about high-valued assets or are we talking about public facing websites with publicly available information, and how we apply the concepts of zero trust are going to be quite different between those environments," he said. "Ultimately, the big questions that came out are: What, if any, changes do we need to look at in terms of our federal approach to information security?"

He said one of the initiatives that rose to the top was the Trusted Internet Connections (TIC).

While the Office of Management and Budget is revamping the TIC policy, Hernandez said the research made it more clear that agencies would benefit from some zero trust use cases under the new guidance.

Kent said the current use cases on the draft TIC policy addresses some parts of zero trust, but OMB also is looking at adding more examples.

"There are multiple layers to look at and how you put those together, in what sequence and in what sequence of maturity, and assessment as a framework to look at your own environment to say 'where am I on each of these pieces?'" she said. "There are a lot of things we want to learn through the small petri dish through the efforts at the council that we can then industrialize and share across all of the agencies for them to use for their own purposes, and then absolutely we'll embed the particular learning and continue to update the uses cases in the TIC policy."

## Identity is a core feature

Another big piece of putting the zero trust framework in place is identity and access management. OMB currently is updating the federal identity management policy—the draft and comments are more than a year old now—but the draft didn't necessarily include any mention or specifically address the zero trust concept.

Kent said that the policy may not need to specifically mention zero trust.

"The zero trust approach is a framework and identity is a component in that. We may put more discipline and detail into identity so we can drive more depth in our algorithms of access at some point in time, and that would go back into the identity policy. But zero trust in itself will not be a component of the policy," she said. "What could be a component of the policy is the identity information and the characteristics that would become a part of what is used in our longer term access and monitoring protocols."

Hernandez added zero trust requires agencies to have accurate, thorough, timely and robust identity and access management information.

"Identity is a core feature of the zero trust mindset. It's so important when we talk about valuable data, we decided in the working group it's not so much who is on the network is so important, but what access to the data do they have? That's the real question," he said. "We started talking about the data layer and how well can we identify folks who are accessing data and understand is that access the right place, right time and right scope, and continuously audit that. Ultimately, if we have high value data, there has to be a

very high level of certainty of the identity that is accessing that. If it's public website and public information, I don't care who is accessing that, anybody can. So drawing those distinctions and having a mature approach to identity management is what allows us to start to enable most, if not all, of the capabilities in the zero trust mindset."

Kent said agencies have made good progress on who is on the network, but most departments still need to improve their understanding of why the user is accessing the data and what they are doing with it. She said getting down to that next layer and being able to track, monitor and determine if it's acceptable is the next focus area.

Kent said OMB and the CIO Council is working with the National Institute of Standards and Technology to assess current state of technology that fits under zero trust framework.

She said OMB also is exploring other areas that may need policy updates to address zero trust concepts.

"This product [white paper] effectively became a baseline as to where we are at in the market and where we are at in the federal space, and it actually generated a plethora of questions that both sides, government and industry, need to come back together to answer and figure out how do we tailor zero trust to optimize our IT and cybersecurity and manage our risk in the enterprise," Hernandez said.