Rebuilding Foundations and Driving Innovation: Insights from Dr. John Zangardi, Former Chief Information Officer, U.S. Department of Homeland Security

By Michael J. Keegan

Editor's Note: *Since this conversation, Dr. Zangardi retired from public service.*

The single most important responsibility of government is securing the homeland—protecting a nation from terrorists and the instruments of terror, while at the same time, fostering the country's economic security through lawful travel and trade. That is the mission of the U.S. Department of Homeland Security (DHS)—securing the U.S. homeland from varied and ever evolving threats. Meeting this mission rests on having in place a modernized and innovative technology and information infrastructure.

Dr. John Zangardi joined me on *The Business of Government Hour* from the 2019 SPADE conference on "Designing for the Future of Defense and Security" from Soosterberg, Netherlands. This year's SPADE conference brought together defense, intelligence, and security leaders from Europe and around the world, in dialogue with experts from industry. At the time of the conference, Dr. Zangardi was the CIO at DHS. He discussed with me the department's IT priorities, and his efforts to modernize its IT infrastructure and change the way IT is done across the DHS enterprise.

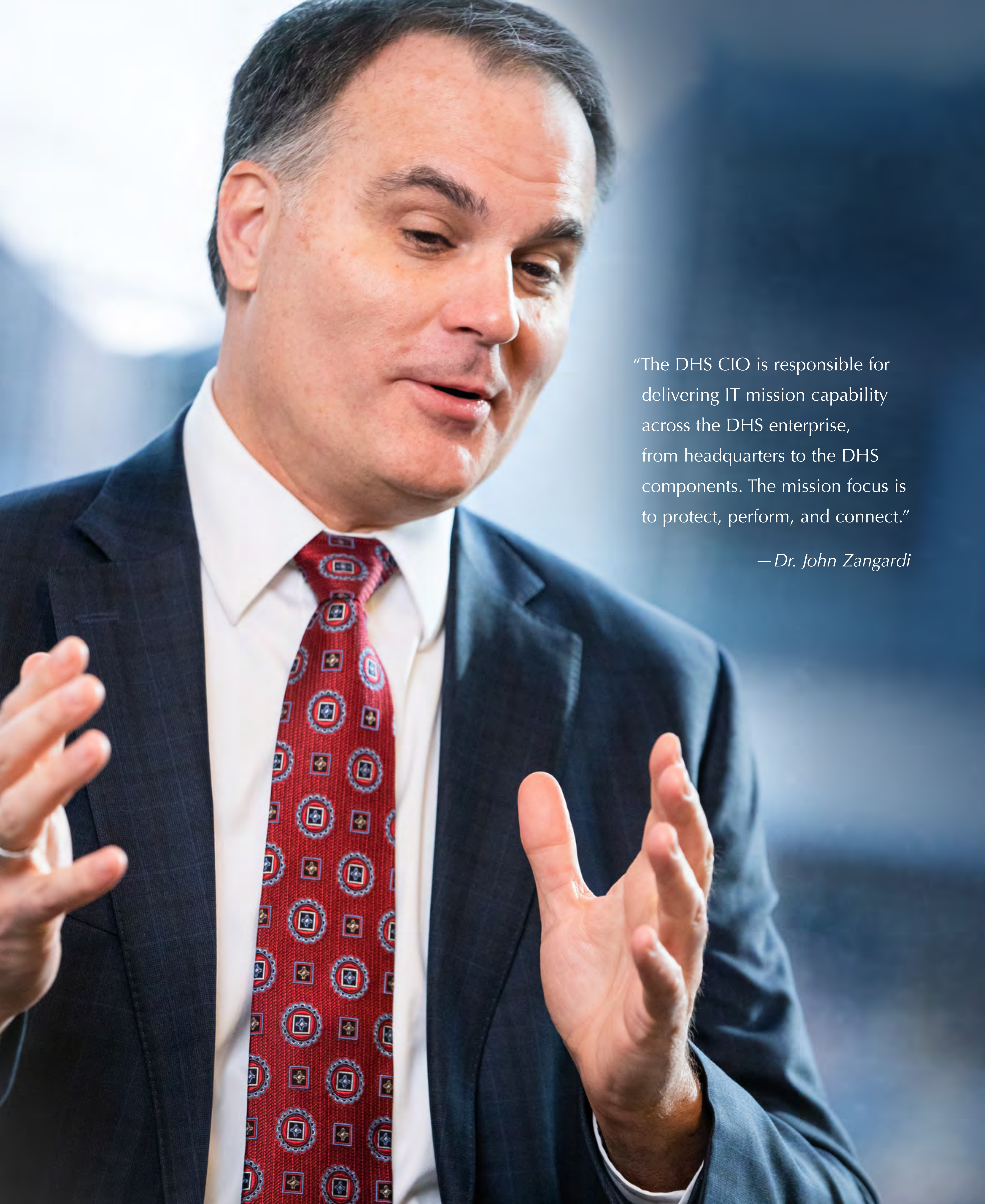
What is the CIO's overall mission at DHS?

The DHS CIO is responsible for delivering IT mission capability across the DHS enterprise, from headquarters to the DHS components. The mission focus is to protect, perform, and connect. Every day requires you have to be on your game—to make sure that the capability people need to do the mission is being delivered. Therefore, you need to efficiently connect the entire enterprise. You need to enable the mission through the movement of data and information across the network. While doing this, you also need to ensure that the system and its contents are protected and secure. For practical illustration, if the need for a new IT capability springs up at the border, the team has to be able to support that quickly. Most important, you have to make sure that what the team delivers can be secured.

The DHS Office of the Chief Information Officer breaks down in several ways. It has an operational component, which is the largest component. The second largest is the security component. There is an area that delivers applications and develops a path to the cloud—assessing how we organize and make better use of our data. There is also an area in the CIO shop that focuses on IT budget. If you don't know where your money is, we cannot protect, perform, or connect functions. Money is the gasoline that makes the engine go.

Along with our operational environment, there is a group that focuses on the future of technology, looking out to see what innovations we can leverage that might be on the horizon. This group also focuses on initiatives like IT modernization as well as handling how we're going to roll out the use of the GSA's Enterprise Information Services (EIS) contract.

In the end, the CIO's mission is to make sure that the DHS components are able to meet their missions. If they need help with something, the CIO needs to make sure that staff is engaging with those components appropriately, in order to get them where they need to be.



“The DHS CIO is responsible for delivering IT mission capability across the DHS enterprise, from headquarters to the DHS components. The mission focus is to protect, perform, and connect.”

—Dr. John Zangardi

"I have learned coming up through the ranks that relationships are everything. The lone wolf theory doesn't work. IT is a team sport. You can't go it alone."
— *Dr. John Zangardi*

What challenges have been faced?

The number one challenge is security. Security breaks down a couple of different ways. You've got to make sure you have a team fully trained and capable of doing the job. We've been focusing on how we train IT security staff and tying it back to something called cyber retention incentive pay. We look at each of the billets that my cyber security team is working in, reviewing their duties and performance, and ultimately, making sure that they are properly trained. We keep them on this track with incentive pay.

Along with securing our systems and infrastructure for today, we also need to anticipate the future of IT security. I participated on a panel discussing 5G, which is a game-changer technology. In light of such an innovation, the key question and challenge is: how do secure the network of the future? We're looking at things like "zero trust identity," how we roll those things out across the enterprise, and how they shape what we're doing. It also requires an attitudinal change. Doing this right goes beyond simply compliance. It goes to truly understanding threats and how they evolve. It's about communicating the threats, the risks, and the potential impact of them to department leadership, so they understand the mission impact if a system goes down.

Speed is a challenge. What I mean by speed is how quickly can we get things out there to people? It is a function of our ability to leverage contracts, resources, and get things built out on the networks. Speed is important because the demand signal today is so much different than the demand signal 10 or 15 years ago. Built into that speed challenge is something that I think is positive within government. Ten, 15 years ago when I was working in business systems, you had a great reluctance to change. Today, that reluctance has waned.

Along with security and speed, the CIO's team needs to possess technical acumen. We are in a very competitive marketplace for talent. People with the right skills—whether in cybersecurity, data science, or the cloud—are in demand. It is a continued challenge to get highly skilled, technical people on board so we can help the department succeed.

How do you lead?

The Navy has a motto: honor, courage, and commitment. I bought into this motto long ago. You need to be committed to what you do every day. A leader must also have courage to do the difficult tasks and the honor to follow through on their commitment. That is, leaders must always, and in every context, maintain their integrity.

A leader must also prioritize. You must limit your priorities while you also empower your staff. Leadership is about, as I said, exhibiting the U.S. Navy motto: honor, courage, and commitment. But it's also about taking seriously the power of delegation.

Would you outline the strategic vision that guided your efforts?

Let's start with my IT priorities. When I arrived at DHS these priorities were made clear to me. My priorities were to modernize the network, secure the network, and deliver capability across the DHS enterprise. We need to modernize the network by taking advantage of GSA's Enterprise Infrastructure Solutions contract vehicle to begin that modernization. It is fundamentally important to how we move forward with our network in delivering new capability at lower cost. Priority number one is getting EIS out the door, on the street, and awarded. At the end of the day, it is about simplifying network management and delivering higher quality performance that ensures information flows smoothly across all DHS missions and devices. This entails maturing a virtual network, exploring mega data opportunities and data portability, accelerating network innovation and agility, and ultimately, enforcing a zero trust network.

Priority number two is in the security field. We are looking to optimize our Security Operation Centers (SOC). SOCs are how we assess and defend our websites, apps, databases, data centers, networks, and desktop computers from cyber intrusion and attacks. Most of the centers operate independently from each other. We have 16 SOCs. We started a long road here in a 'crawl, walk, run' strategy. We're beginning to get into our 'walk' phase. The SOC optimization is part of a wider DHS effort to simplify and amplify cybersecurity. That effort involves contracting, operations, and tools, such as Continuous Diagnostics and Mitigation (CDM). We have delegated aspects of the optimization effort to component chief information security officers (CISOs). The Customs and Border Protection (CBP) CISO has the lead for identifying what tools we want to have on our network. The Immigration and Customs Enforcement (ICE) CISO is focusing on policy and procedures. Across tools and procedures, we have to recognize that DHS components may have uniquely different missions and we need to make allowances for those differences, ensuring that we don't make it harder for them to achieve their missions. The Secret Service has the lead here. It has been developing the single multiple award contract that will provide a central pool of services from which all DHS SOCs can pick and choose.

Another key priority focuses on department and component data. We completed a study exploring how to instantiate a DHS chief data officer. Is it a CDO policy? Is it a CDO with a lot of authority? What is it? That is the problem we've been wrestling with. We have also laid out an intelligent automation strategy that deals with robotic process automation, machine learning, and artificial intelligence (AI). We're not going to jump immediately to AI. We'd probably fail. It is about: how do you start small and then build your way up to AI? We're focusing this effort on mission-support aspects of DHS—the business systems.

We are also working on reducing our data center footprint as much as possible. Doing this gets down to cost versus mission. Getting to the cloud is also important for us. It enables us to meet our missions by enhancing our mobility. We have got to make sure that the right security is in place when we do it. My strategy on cloud has always been federated hybrid. We're not going to pick just one. We're going to go with whatever makes sense based on cost, schedule, and performance. What is the capability I get? What's the cost? How quickly can I deliver it? All critical questions guiding how we move to the cloud.

From your perspective, how has the role of the CIO within federal agencies changed over the years? What characteristics make one a successful CIO?

I have learned coming up through the ranks that relationships are everything. The lone wolf theory doesn't work. IT is a team sport. You can't go it alone. If you look at game theory, trust is built on probability of defection, right? You want people to understand that when the time gets tough, you aren't going to defect. I am in there with you. Building that trust—where people know they can rely upon you—leads to collaboration and greater success.

I have had three federal CIO jobs, all dramatically different. The Department of Navy CIO was very policy focused with an enterprise perspective and not much focus on actual execution. As the acting Department of Defense CIO, you focus on policy, but you have a lot of overarching work that you need to do with the military services, pulling them together. You are very involved in spectrum. You are very involved in military satellite and nuclear command and control communications. Moving to the DHS CIO, it is a very IT mobility focused organization, where the priority is on execution and getting the right things out there. Albeit three very different CIO jobs, but when you look across the variances, there is one characteristic needed to be successful. Can you build relationships? Can you understand the other person's problems? Are you going to help them get through those problems? When you think about the characteristics of a CIO, if you want to drive change, you need people to trust you. You've got to have established relationships.

What advice would you give someone who is thinking about a career in public service?

Just do it. It is wonderfully rewarding. You will get back more from public service than you will from anything else. It's hard. You have to come into it with the realization that it is not going to be the easiest thing that you've ever done, but it is really worthwhile.

To learn more about the U.S. Department of Homeland Security, go to dhs.gov.

To hear the interviews from *The Business of Government Hour*, go to businessofgovernment.org/interviews.

To download the show as a podcast, go to PodcastOne or iTunes and search for *The Business of Government Hour.*

To view excerpts of the show, go to youtube.com/businessofgovernment.