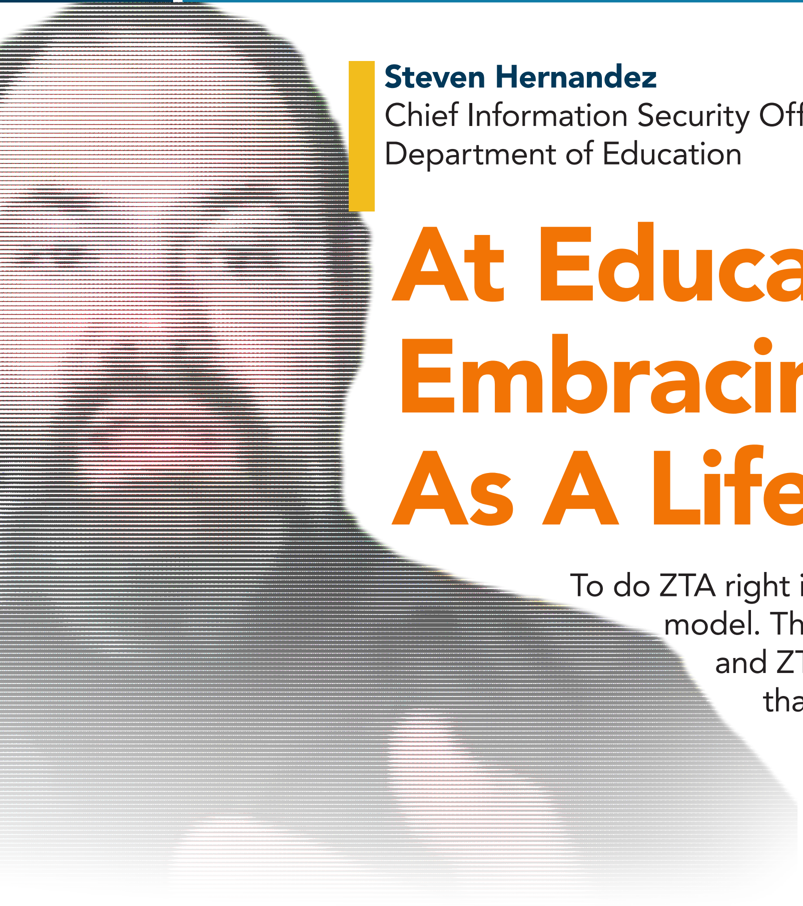


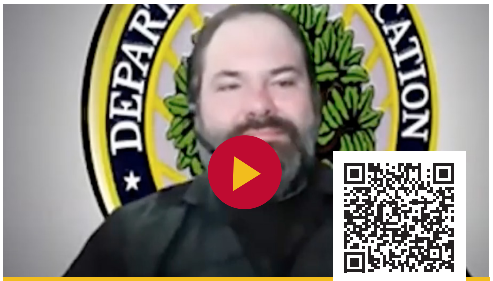
Steven Hernandez
Chief Information Security Officer (CISO)
Department of Education

At Education, Embracing Zero Trust As A Lifestyle

To do ZTA right is to touch every element of the 7 layer model. That's not just networks, that's an architecture and ZTA had to evolve to be more encompassing than Zero Trust networks.

Progress On ZTA's Four Pillars

Almost three years ago the CIO Council decided to explore Zero Trust networks. The first request was to focus on Layer 3 and see what was "the art of the possible." We pulled together government focused working groups with our friends at the NIST Cybersecurity Center of Excellence and ACT-IAC. We soon realized this is much bigger than Layer 3 and to do this right we really have to talk about the whole 7 layer model and touch every single element of it.



Mr. Hernandez comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

That's not just networks, that's an architecture; and that's how we landed on Zero Trust Architecture (ZTA) versus something like Zero Trust Network. We had to evolve it to be more encompassing. At the department we have four big pillars:

First, we are looking at data both knowing what those crown jewels are; and collecting the data necessary from our fabric of sensors throughout the enterprise to know what is going on around us.

Second, we have ICAM (Identity, Credential, and Access Management) identity which is absolutely core to what we're doing, but there are other elements in identity that we're still looking at building out – especially around non-person entities.

Then we have the trust engine which is an area we are pushing hard. We're looking at the Technology Modernization Fund as a way to take advantage of some of the cool technology that's out there such as AI, AML, Robotic Process Automation; and bring it in from an enterprise perspective across the entire enterprise which is frankly really hard to do. Lots of ZTA solutions out there do have elements of machine learning and AI built into that particular product space or service space. But is it enterprise-wide and can it co-mingle with other things? There are various degrees of capability there.

Finally there is that control fabric, the control plane and that's another area of work for us that we're driving hard; it's probably the most nascent on the horizon for us because we just awarded EIS (Enterprise Infrastructure Solutions) and we're getting lots of incredible technology through that service offering.

Profile Of A ZTA Lifestyle

ZTA is a "lifestyle"; I think I am safe in saying that Zero Trust is the pursuit of perfection; and we will likely never get there, but we're going to pursue the hell out of it until we get as close as we can.

> ZTA is a "lifestyle"; I think I am safe in saying that Zero Trust is the pursuit of perfection; and we will likely never get there, but we're going to pursue the hell out of it until we get as close as we can.

With data, when we look at Zero Trust from the cybersecurity perspective, we knew even a data warehouse was not going to be sufficient for us over the next five, ten years when it comes to ZTA.

So over two years ago we started building a cyber data lake; the whole concept being that we want the native data in its raw format (accurate, thorough and timely) to be in our data lake or accessible by our data lake in a data lake fabric. We've made some good architectural decisions building in the ability to grow, so elasticity is not an issue.

The other part we are looking at how do we then make use of all that data. We are doing some pretty cool stuff with our human skill sets as well; we're bringing on actual data scientists into our security operations space, because they're going to be the ones who are going to help us train the machines later. But first they need an idea of what data we have, what it looks like, where there might be nuances to that data. Then where do we need to build out a data warehouse-like capability?

As we bring on additional Zero Trust capabilities they have to feed into that ecosystem to be able to leverage what's in that ecosystem. We call this our Data Dominance Initiative.

Priorities: SASE and SOAR

The real opportunity on the horizon is around a Secure Access Service Edge (SASE) and Security Orchestration and Automation Response (SOAR) especially as it relates to our security operation. Combined these two areas make about 90% of ZTA a real possibility.

We're really talking two areas: (1) the idea of the control plane and that's where a lot of that SASE technology comes in. The important part about the SASE technology is how it relates to how we move the Trusted Internet Connection (TIC) into the cloud. Really we're talking about SASE and talking about moving the idea of a tie-cap, which is a physical construct into a virtual concept which is now going be in the cloud. That's just a fundamental game changer. Combine that for example with some the endpoint client technology where the end user is no longer using a VPN they way they think because that client on the endpoint is going to handle almost all the encryption and it's going to be done without their involvement or interaction.

Wow! What a win for the end user and that's really how we start selling Zero Trust as it's not only good for the goose and the gander, it's going to make your job better and easier because a lot of the security interruptions that you feel you may have now they are frankly going to fade away.

On the source side that gets into that trust engine discussion and how do we really start the orchestration and automation of actions starting in the Security Operations Center.

When we talk about SOAR and SASE, those are the capabilities that we are bringing to the forefront; and for us in the next two-three years that's what we are really going to be driving hard on. ■