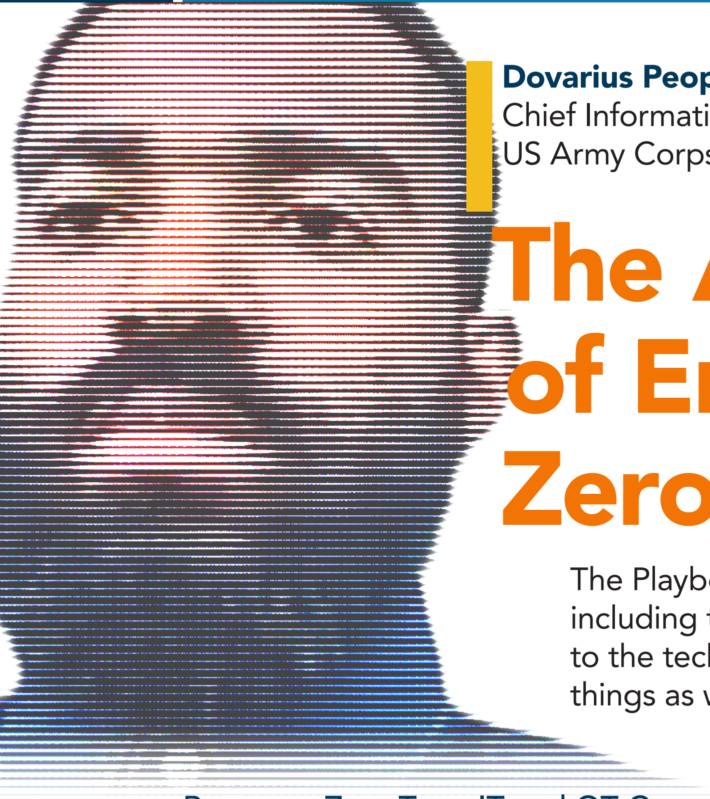

Dovarius Peoples
Chief Information Officer (CIO)
US Army Corps of Engineers

The Army Corps of Engineers' Zero Trust Playbook

The Playbook playbook goes through 12 different areas including the training aspects from the executive level down to the technician that is responsible for implementing those things as well.

Progress: Zero Trust IT and OT Controls Into Next Generation Firewalls

Things were progressing on Zero Trust before the Executive Order came out. We've already had good conversations with the Federal CIO Council members on Zero Trust and internally in the Department of the Army.

We have developed what we call the Zero Trust Playbook. The Playbook playbook goes through 12 different areas because when most people talk about Zero Trust they only talk about it from about three different perspectives. But we have gone through it from all aspects of Zero Trust to include the training aspects from the executive level down to the technician that is responsible for implementing those things as well.

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

Because ultimately in order to implement and execute Zero Trust, you have to be trained and we have put a heavy emphasis on the training of our personnel. Another thing we have done is look at Zero Trust from the perspective of not IT, but operational technology (OT) as well because the Corps has a heavy civil mission and that civil mission includes working with a lot of the levees, locks and dams at the local state level.

We support those state levels when it comes to disaster recovery, waterway missions and critical infrastructure and those type of things. This is one area that we believe could be enhanced with Zero Trust even as we work to meet the Executive Order that was published. So we are looking at this from all aspects – OT, IT – and how do we implement our Zero Trust framework through a playbook and that playbook also constitutes training as well.

Success: From Conceptualization To Operationalization

One of the things we have to do at the Corps is emphasize how we meet the end user where they are. How do we meet that engineer at a distant site enabling them to do their mission effectively and efficiently? Ultimately IT from our perspective is an enabler; so a lot of time we use a lot of technical terms and we talk a lot of technical language, but the end user says "what does this mean to me?"

So we begin to take the conceptual aspects of Zero Trust and begin to operationalize that concept. With

with that being said, from a DOD perspective many are probably aware of the CVR (Commercial Virtual Remote) environment that was just was recently decommissioned due to the fact that we're beginning to modernize and think a little bit differently. But the CVR is a great example of how we operationalize the Zero Trust methodology and concept due to the fact that with Microsoft Teams capability, it enables collaboration or mission collaboration to an end user through a mobile device. That means you can do your job from anywhere effectively and collaborate efficiently with anybody whether that is the Department or in the federal space DOD and non-DOD entities.

Whether you were Air Force, Army, Navy or throughout DOD, you had the ability to connect with all your partners. That means being able to deny all except those allowed by exception; partitioning to allow for those that need access to their mission critical data, mission critical elements; and being able to have good access to view and receive those logs and communicate externally with vendor partners to be able to secure that information as well. So that is a good example of how we operationalize the concept of Zero Trust to enable the end user to effectively be able to perform their mission.

> Ultimately being able to access critical information through a mobile device – whether you are sharing it with other mission partners or using it internally – is the goal.

Then again we are also looking at it from the perspective of OT. When you think about construction, being able to build different buildings and you have Wi-Fi sensors and all those other things inside of the enterprise, you have to be able to deploy some Zero Trust principles in order to ensure that those OT capabilities are properly secured as you transfer buildings over to different customers.

So, we have done a lot in that space and continue to lean forward, learn and grow. But we have to begin to execute on the Zero Trust principles and not just theorize conceptually about some of those things as well.

Priority: Continue Our Digital Transformation Journey

We are continuing with that same theme we've had of meeting the end user where they are. But there are several critical priorities that we are beginning to put focus on: one is the leveraging of shared services.

When you talk about Zero Trust you think about shared services and the federal government. That's one of the things I personally believe that from a federal DOD-side of the house, we could do a lot better job of leveraging some of the things our brethren in other organizations have done. And using Zero Trust to ensure that it's properly secure so leveraging that capability to help empower the end user.

In order to be a really world-class organization – which we continue to emphasize in the Corps – that digital transformation journey is very critical and key. Zero Trust is an enabler of mission effectiveness and efficiency; so being able to secure and protect all by leveraging a lot of other good cyber practices such as continuous monitoring and those types of things.

I think last but not least is we're putting a lot of emphasis on the data modernization, data strategy journey. Ultimately being able to access critical information through a mobile device – whether you are sharing it with other mission partners or using it internally – is the goal. Being being able to secure that data through the Zero Trust methodologies and principles allows us to be a lot more efficient when it comes to meeting mission goals and objectives.