Accelerating Mission Outcomes through Zero Trust

David M. Wennergren
CEO, American Council for Technology & Industry Advisory Council (ACT-IAC)

"Only trust thyself, and another shall not betray thee." William Penn. As John C. Maxwell pointed out, "progress does not occur without change," and change inevitably brings both opportunity and risk. One of the top risks we currently face is the ever-increasing threats to our networks and data. Go to any news source and the headlines trumpet the headaches that technology leaders face daily—Solar Winds, Colonial Pipeline, ransomware, phishing attacks—the list goes on and on. William Penn may have spoken a truth about trust, but it does seem to be a negative view for us at a time when collaboration and information sharing is a key to success in both business and government. Indeed, as a technology leader, if we follow Penn's quote to its logical conclusion, we may be inclined to so lock down access to our networks and systems to prevent malware from taking root, that we also impede the flow of knowledge in to and out of our organization—in a sense, we create a self-inflicted denial of service attack. Fortunately, there is another path.

"Trust is the glue of life." Stephen R. Covey. Zero Trust has generated a lot of interest recently as a key tool in reducing cybersecurity risks while still enabling information sharing and legitimate access. In the old world of on-premise enclaves, a network perimeter-based protection scheme was a logical choice. However, as we moved into a cloud-based, mobile access, virtual work environment world, it became crucial to shift away from a security strategy that may have made initial access hard, but once gained, allowed unfettered access to everything within a network.

Zero Trust uses a combination of robust identity management, access control, data-level security and strong monitoring to create an environment where positive identification and authorization allow transactions to occur—enabling access to trusted entities while simultaneously preventing access by untrusted individuals.

A couple of years ago, the U.S. Federal CIO Council asked the American Council for Technology and Industry Advisory Council (ACT-IAC) to evaluate the maturity and availability of Zero Trust for federal agency adoption. The government and industry volunteers at ACT-IAC responded with two reports.

The first report, *Zero Trust Cybersecurity Current Trends* identified foundational concepts, strategies, and challenges. Key findings included:

- Zero Trust adoption does not require a wholesale replacement of existing networks or a massive acquisition of new systems, and many organizations already have in place some of the building blocks for Zero Trust.
- Zero Trust solutions are available and in use in the private sector.
- Zero Trust efforts require a combination of poli-

Zero Trust principles not only help to reduce cybersecurity risks, but also help to ensure that we accelerate, rather than impede, the legitimate flow of knowledge.

cies, practices, and technologies to succeed.

- Organizations should have a solid handle on their people, assets, data and associated business processes to implement Zero Trust.
- Many cybersecurity professionals endorse Zero Trust as an effective approach to strengthen protection against current threats.
- Success at Zero Trust does require a "whole of agency" effort and commitment from both the technology team and mission owners.

The second report, *Zero Trust Report: Lessons Learned from Vendor and Partner Research*, highlighted available products, solutions and use cases, all aligned with National Institute of Standards and Technology (NIST) standards and Department of Homeland Security guidance—a reminder that you're not alone, and that there are new products, repurposed existing products and a number of "lessons learned" that you can take advantage of in deploying Zero Trust. Both reports are available at www.actiac.org.

"Love all, trust a few, do wrong to none." William Shakespeare. Cybersecurity remains a national imperative, with the intellectual capital and competitive advantage of our Nation at stake. As we replace aging legacy infrastructure and systems, it is crucial that we embed cybersecurity tools and best practices from the start, rather than as an afterthought. It's also crucial that as we emerge from the pandemic, we ensure that we don't just observe the changes we've faced, but instead learn from them. Recognizing that the changing way we do business demands new cybersecurity approaches, Zero Trust principles not only help to reduce cybersecurity risks, but also help to ensure that we accelerate, rather than impede, the legitimate flow of knowledge, both within our organization and with our customers and mission partners. ■

About The Author

Mr. Wennergren is the CEO of ACT-IAC, the national non-profit public-private partnership dedicated to advancing the business of government through the application of technology. He has extensive leadership experience in information technology and change management and has served in a number of senior positions, most recently in the private sector as a Managing Director at Deloitte Consulting LLP, EVP & COO at the Professional Services Council and a VP at CACI International Inc., and prior to that in government as Department of the Navy CIO, Vice Chair of the Federal CIO Council, DoD Deputy Assistant Secretary of Defense/Deputy CIO and DoD Assistant Deputy Chief Management Officer. He is also a fellow and chair of the board at the National Academy of Public Administration.