SSCs Zero Trust Cyber Effort Has Mission in Mind

Published March 27, 2024
By SSC Public Affairs

EL SEGUNDO, Calif. -- You've been hacked!

In today's digital world, these words send a chill through everyday users and pose major threats to our Nation's infrastructure. As expressed in a 2021 Executive Order from The White House, the harsh reality is that the United States "faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."

Taking bold steps to protect our Nation's space-enabled capabilities from cyber vulnerabilities and/or attack, Space Systems Command (SSC) is partnering with industry to develop and integrate a Zero Trust security architecture across the entire space operational enterprise, from terrestrial assets to orbiting satellites and everything in between.

Leading the effort is Col. Craig Frank, SSC's chief information officer.

"With foreign adversaries developing capabilities that threaten U.S. space operations, securing the future of space is one of the most urgent priorities of our time," said Frank.

Near-peer competitors and adversaries are relentlessly conducting malicious cyber activity across all sectors of U.S. infrastructure, exploiting valuable data systems; and they have demonstrated the ability to deny, disrupt, degrade, destroy, or manipulate vital information and networks during conflict. These cyberattacks are often executed with a high level of sophistication and involve the theft of valuable intellectual property, potentially compromising the security of space-based communications, navigation, and reconnaissance systems.

As SSC's CIO, Frank is the senior Information Technology advisor to the Commander, SSC. He oversees various national security and defense business systems -- managing information resource and identifying efficiencies. As CIO, he is also responsible for matters relating to the Command's information enterprise: Cyber, Data Fabric, Information Technology, Network Infrastructure, and Software.

As defined by executive order, a Zero Trust security architecture "eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."

The model recognizes that insider threats continue to be the number one cybersecurity threat, with an estimated 85% of all data breaches involving some sort of human interaction. The next major threat is third party exposure, in which cybercriminals can many times gain privileged accesses to their primary target through the hacking of less-protected third party networks.

In Zero Trust Architecture, users only have access to the bare minimum of what they need to do their jobs. This limits the potential damage in the event that a device is compromised or nefarious access is gained.

In August 2023, SSC awarded a $17 million contract to Xage Security to tailor a strategic "Never Trust, Always Verify" cybersecurity model to systems and assets developed and managed by SSC. In support of the Presidential 2027 Zero Trust mandate, the CIO's office actively identifies and supports system owners desiring to enhance the security of their legacy systems. Systems owners are encouraged to leverage a comprehensive Identity and Data Access Management system offered under this contract. Interested parties within SSC engage as customers and benefit from advanced protection measures tailored to their needs.

“It’s important that we start actively working towards a flat, Zero Trust network that will protect our information without hindering its effective usage,” Frank said. “This effort supports secure interactions between defense and commercial ground and space assets while protecting sensitive information.”

The DoD-mandated program is an essential step towards cyber-hardening terrestrial-based systems, including ground stations and operational technology assets, and extending these capabilities to next-generation ground and space systems. Ultimately, the effort aims to prioritize data integrity, confidentiality, and authenticity across all layers of the space ecosystem.

“This is a unique opportunity to contribute to a resilient cybersecurity architecture, shaping the future of secure data exchange and protection in complex distributed environments,” said Frank.

“We recognize we’re going to need everyone at SSC to understand not only how Zero Trust works, but why it is critical for national security and defense,” Frank said. “We also want to hear feedback and comments in order to make sure we’re not overlooking any concerns or questions about how this will be implemented, and how it will affect the mission.”

For inquiries about Zero Trust, and for cyber leads and engineers interested in participating in the Zero Trust pilot program, please contact SSC.CIO.FrontOffice@spaceforce.mil.

Originally published on United States Space Force Space Systems Command online Newsroom.