AN OFFERING IN THE BLUE CYBER SERIES:

# Small Business Zero Trust Steps

## VERIFY EVERY TIME

Version 14 March 2022

#18 in the Blue Cyber Education Series

# There is NO Zero Trust Requirement in your Small Business Contract

- This Briefing is in response to questions about how Zero Trust applies to DAF Small Business Contractors.
- The DOD and DAF are implementing zero trust on their information systems and large networks.
- This information is just to keep you up-to-date on another philosophy which can influence your cybersecurity decisions.

# Defining Zero Trust

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

- This definition focuses on the crux of the issue, which is the goal to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible.
- That is, authorized and approved subjects (combination of user, application (or service), and device) can access the data to the exclusion of all other subjects (i.e., attackers).
- To take this one step further, the word “resource” can be substituted for “data” so that ZT and ZTA are about resource access (e.g., printers, compute resources, Internet of Things [IoT] actuators) and not just data access.

# What is Zero Trust?

- Zero Trust is not the security of the past. Traditionally, a '*castle and moat*' paradigm, is an information system architecture designed to create an impenetrable perimeter and allow no unauthorized access. Your network is protected from bad guys and you can rest assured. Or can you? Just because you know everyone who comes in – can you trust them? And from this question… Zero Trust was formed.
- Today's networks don't have clear boundaries. Your network is all over the map, some parts in the cloud and some on premise. Some teammates are virtual and some are standing across the room. Your sensitive government data and intellectual property may be mixed. `The modern network does not have clear boundaries. Your HR Team uses a SaaS, your programmers work from home and you have no idea who maintains the facilities. You can't create a moat when your castle is the globe.
- Zero Trust protects your data and resources no matter where your assets are or where your users are.

Caerlaverock Castle, in Scotland. (Wikimedia Commons Photo / cc2.0)

# Zero Trust in Action

- The Zero-Trust security model is designed with the idea that your adversary is already in your network and that your network is not secure, no matter what you have done to protect it.
- The objective then, is to control access by making access to data very specific and short-lived.  In Zero Trust, the combination of user, application, service and device are granted time-limited access to data.
- Federal agencies of the U.S. government have been encouraging organizations to adopt a security model based on Zero-Trust principles for over ten years,
- The initial step should be on restricting resources to those with a need to access and grant only the minimum privileges (e.g., read, write, delete) needed to perform the mission.

# The principles of the Zero Trust

- **Ensure that data is accessed securely regardless of its location:** Any connection to data must be proved safe, regardless of where it is made from.
- **Adopt the "least privilege access model" strategy and enforce access controls:** An user should be given access only to the resources they need to perform their job and prevented access to the rest.
- **Inspect and monitor everything:** Activity should be inspected not only at the network access point but also inside the network, trying to identify unexpected behavior.


AFWERX SBIR ★ STTR

# THE PRINCIPLE OF LEAST PRIVILEGE

The principle of least privilege defines any user, program, or process should have only the necessary minimum privileges necessary to perform its function. The principle of least privilege can also be referred to as the principle of minimal privilege or the principle of least authority.

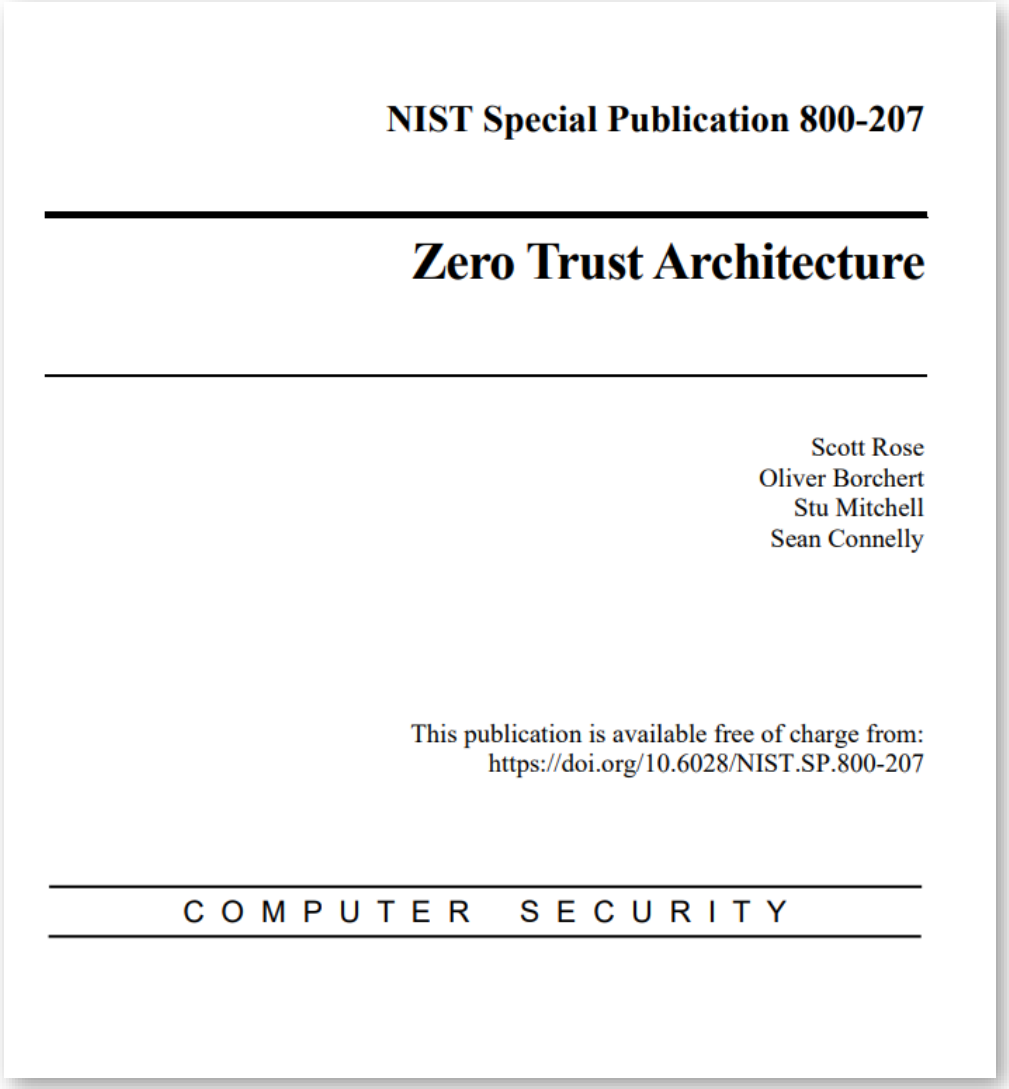
The principle of least privilege works by allowing only enough access to perform a task. Implementing the principle of least privilege reduces the risk of threat agents gaining access to critical systems or sensitive data via taking control of a general user account, device, or application. Using the principle of least privilege helps contain bad actors to their area of access, stopping them from moving to the system at large. Following the principle of least privilege is considered a best practice in information security.

# Tenets which define Zero Trust (NIST)

- All data sources and computing services are considered as ‘resources’
- All communication is secured (internal or external)
- All access is provided ‘per-session’
- Access is provided based on a dynamic risk-based policy
- All devices should be in the most secure state possible. They should be monitored for this
- Dynamic authentication and authorization is strictly enforced before granting access
- Collect as much information about the network and infrastructure as possible

# NIST SP 800-207
# Zero Trust Architecture

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf



NIST Special Publication 800-207

Zero Trust Architecture

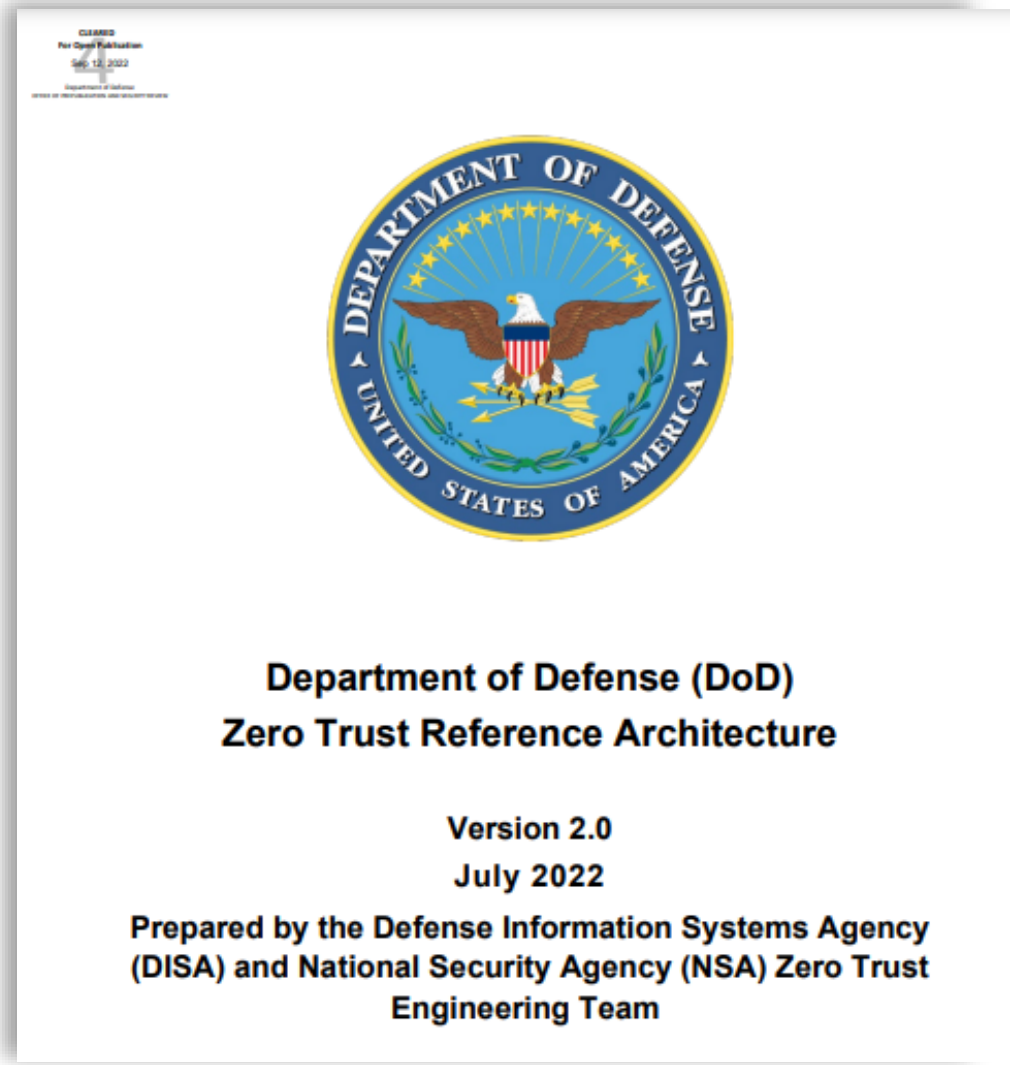
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

# Department of Defense (DOD) Zero Trust Reference Architecture

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf



Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022

Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

# Key steps already in NIST SP 800-171 for a Zero Trust approach

These steps below will allow small businesses to take a Zero Trust approach to cybersecurity and data protection

## 1) Continually monitor and audit all user account access.

**Always know who is using your company's network, when, how and for how long.** Limiting access on all these points to short sessions will ensure proactive enterprise risk management. You already accomplish this step with NIST SP 800-171 implementation of System Integrity 3.14.13, 3.14.6; Security Assessment 3.12.3; Identification and Authentication 3.5.4, 3.5.3; Audit and Accountability 3.3.1, 3.3.2; Access Control 3.1.6, 3.1.12, and lastly, 3.1.5 "Employ the principle of least privilege, including for specific security functions and privileged accounts."

## 2) Regularly update passwords to prevent a privileged access data breach.

**Good password management is invaluable** for your enterprise cybersecurity. If you have accounts that have access to valuable intellectual property or customer data, then securing them behind a solid password is essential. Make sure that access is only granted to users who are thoroughly identified before any login credentials are released. You already accomplish this step with NIST SP 800-171 implementation of Identification and Authentication (3.5.7 through 3.5.10).

## 3) Ensure two or multi-factor authentication is used by everyone.

**Every employee, contractor, partner, or admin account must authenticate**. Making sure that multi-factor authentication is used is a key preventative step. With this step you will reduce the opportunity for a attackers to gain access to privileged accounts. You already accomplish this step with NIST SP 800-171 implementation of Identification and Authentication 3.5.3 and Maintenance 3.7.5)

# Key Steps Continued

## 4) Utilize privileged access credentials to all network devices

**Change immediately any manufacturer preset passwords or login credentials.** These are a known cause of data breaches and malware events. You already accomplish this step with NIST SP 800-171 implementation of Identification and Authentication 3.5.3, 3.5.4, and Access Control 3.1.6, 3.1.5, 3.1.7, 3.1.15.

## 5) Make sure all remote access is secure across all employees and contractors, regardless of where they work.

**Remote access must be restricted and monitored.** It is a source of issue for small businesses. Unsecured Wi-Fi can become on ramp for attackers to access your systems. A VPN is better than nothing, but the bad guy could be inside your VPN! Secure open IoT networks behind SSL certificates is a must. You already accomplish this step with NIST SP 800-171 implementation of System and Communications Protection 3.13.7 and 3.13.12 as well as all the Access Control 3.1.12, 3.1.13, 3.1.14, 3.1.15.

# Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security / data protection questions to https://www.safcn.af.mil/Contact-Us/