NSA GUIDANCE · OPERATIONAL TECHNOLOGY

Zero trust for the shop floor

What NSA's new OT guidance means for small and midsize defense contractors, and where to start.

WHAT NSA RELEASED

On Oct. 8, 2026, NSA published a Cybersecurity Information Sheet, *Hardening Department of War (DoW) Critical Operational Technology (OT) Environments with Zero Trust (ZT) Principles*. It applies zero trust to controllers, plants and facility systems despite their technical limits.

THE CORE IDEA

"Never trust, always verify."
Assume an attacker may already be inside. Verify every user, device and connection, and limit how far a breach can spread.

Where to start

Our practical reading for shops that run or support equipment, controllers, labs or facility systems.

01	**Map what you have**	List controllers, engineering workstations, vendor accounts and remote access paths, and anything exposed to the internet.
02	**Gate remote access**	Take OT off the open internet. Require named accounts, strong authentication, approval and time-limited sessions.
03	**Separate OT from IT**	Segment the shop floor from business systems and allow only the traffic each machine actually needs.
04	**Shield legacy equipment**	Harden what you can. Where an older device can't be patched, protect it from the outside with network controls.
05	**Monitor without disruption**	Review logs, prefer passive monitoring, and test changes so they never interrupt sensitive equipment.

How this relates to CMMC Level 1

NSA's OT guidance is

- Security advice that strengthens your overall posture.
- **Not** a new CMMC requirement or a substitute for your self-assessment.

CMMC Level 1 is

- The **15 safeguards in FAR 52.204-21**, for systems that handle Federal Contract Information (FCI).
- An **annual self-assessment and affirmation in SPRS** when your contract requires CMMC. Handle CUI? Check whether Level 2 applies.

SCAN&ACT · CMMC LEVEL 1

Know where you stand before your next contract.

Scan&Act walks you through all 15 Level 1 safeguards in plain English, flags gaps and shows what to fix. The assessment is free; get the document pack when you're ready to affirm.

Start free assessment →

federalshield.tech

Sources: NSA press release and CSI, Oct. 8, 2026 (nsa.gov) · FAR 52.204-21 · DFARS 252.204-7021 · 32 CFR Part 170.

FederalShield is independent and is not affiliated with or endorsed by NSA or the Department of War (DoD). This brief is general information, not legal advice.