

NSA Releases Zero Trust Guidance for Protecting Operational Technology Systems

Datum 9.10.2026
Subjekt National Security Agency / Central Security Service
Region USA
Kategorie IT-Industrie, Staatliche Institutionen, Sicherheit

FORT MEADE, Md.—Today, the National Security Agency released a Cybersecurity Information Sheet (CSI), “Hardening Department of War (DoW) Critical Operational Technology (OT) Environments with Zero Trust (ZT) Principles.”

The guidance recommends using ZT mitigation principles to prevent catastrophic impacts to U.S. national security, economic security, and public health and safety. While primarily intended for National Security Systems (NSS), DoW, and Defense Industrial Base (DIB) network system owners, and the operators responsible for protecting these critical systems, this guidance is also applicable to technical leaders and experts, as well as information technology and OT managers and administrators.

ZT assumes the occurrence of adversarial breaches and uses a “never trust, always verify” principle. By assuming compromise is possible or already present, ZT continuously verifies users, devices, workflows, and communications. Applying these principles to OT strengthens protection against unauthorized access, lateral movement, and adversarial persistence.

The adoption of ZT principles is essential for enhancing the security of legacy OT, enabling defense-in-depth across critical infrastructure while ensuring adherence with federal guidance.

While organizations are increasingly integrating super intelligence (SI) into OT to improve efficiency, resilience, and mission effectiveness, this introduces new risk, attack surfaces, and disruption opportunities. Adversaries are leveraging SI capabilities to automate reconnaissance, accelerate exploit development, and conduct cyber campaigns at unprecedented speed and scale, making achieving ZT outcomes on OT systems more critical than ever. Adversarial attacks now extend beyond espionage and reconnaissance, often aiming to deny, degrade, disrupt, deceive, or destroy the United States’ critical infrastructure. The consequences of such attacks vary by sector and can result in significant and widespread damage. Affected sectors may include, but are not limited to, energy, water, agriculture, public health, and government facilities.

Read the report and visit our [full library](#) for more cybersecurity information and technical guidance.

NSA Media Relations
MediaRelations@nsa.gov
443-634-0721

[About the National Security Agency](#)

The National Security Agency leads the U.S. Government in cryptology that encompasses both foreign signals intelligence (SIGINT) insights and cybersecurity products and services and provides the Nation decision advantage in competition, crisis, and conflict.

###

<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4621936/nsa-releases-zero-trust-guidance-for-protecting-operational-technology-systems>