NNSA Comprehensive Cyber Assurance Strategy

One of NNSA's core missions is to maintain a safe, secure, and reliable nuclear stockpile. To achieve this, NNSA employs *Nuclear Enterprise Assurance*, a program designed to prevent, detect, or mitigate threats to U.S. nuclear weapons and their enabling capabilities.

What is the Comprehensive Cyber Assurance Strategy?

Developed to strengthen the countersubversion mission, this strategy is a coordinated approach to identify, assess, and mitigate cyber risks across both Operational Technology (OT) and Nuclear Weapons Information Technology (NWIT) environments.

Operational Technology

Physical systems vital for designing, building, and testing nuclear weapon components.

NW Information Technology

Information technology systems integral to proper operation of a nuclear weapon's core functions.

Subversion & Sabotage

Malicious activities that are intended to degrade or disrupt weapon reliability & performance.

The Role of "Assurance"

Verifying integrity of U.S. nuclear weapons & their processes, from design to decommissioning.

Why is this Strategy Crucial?

Mitigating Cyber Risks

This cohesive, 10-year cyber assurance strategy **bolsters inventory system security** by comprehensively identifying, assessing, and mitigating cyber risks, safeguarding against potential compromise from design through suststainment.

Addressing Aging Stockpile Technologies

Many U.S. stockpile weapons date from the 1970s-80s, predating significant digital integration. As components are updated, stringent measures ensure **all new technologies are securely incorporated**, maintaining integrity.

Managing Risks Holistically

OT risks are managed via tailored cybersecurity and physical controls, **prioritizing performance, reliability, and safety.** NWIT risks utilize robust **Systems Security Engineering**, leveraging NNSA's rigorous engineering & cyber processes.

★ **Nuclear Enterprise Assurance: Integrity by Design** — Integrity is embedded throughout the systems engineering lifecycle—from initial design, through production, sustainment, modernization, and retirement. This ensures that assurance is a fundamental part of the process, not an afterthought.

★ **Investing in the Future of Security** — For over 30 years, the U.S. has invested in advanced experimental facilities, modeling and simulation tools, and cutting-edge technologies to ensure stockpile reliability. *NNSA's Comprehensive Cyber Assurance Strategy* builds upon this foundation, adding another vital layer of security to affirm the credibility and dependability of the nation's strategic deterrent.