EXECUTIVE BRIEF

Preparing for NSPM-12

From Compliance Mandate to Mission Strategy

Building a Trusted Data Foundation for National Security Systems: A Joint Point of View from Hitachi Federal and Denodo

National Security Presidential Memorandum 12 (NSPM-12) marks one of the most significant shifts in cybersecurity governance for National Security Systems (NSS) in decades. Rather than introducing a single technology requirement, the memorandum establishes a government-wide framework for improving cybersecurity accountability, strengthening governance, modernizing policy implementation, and enabling secure collaboration across agencies responsible for our nation's most sensitive missions.

For agency CIOs, CISOs, mission owners, and cybersecurity leaders, the immediate challenge is not selecting new technologies, it's developing a practical roadmap. Agencies must understand their current environments, identify gaps, establish governance, and determine how existing investments can support evolving CNSS directives while preparing for future requirements.

Organizations that begin planning now will be positioned to move faster as guidance evolves and funding becomes available.

Why NSPM-12 Matters

NSPM-12 is more than a cybersecurity directive. It establishes a new governance model designed to improve how National Security Systems are managed, protected, and operated across the federal government. Among its priorities are:

- Modern cybersecurity governance for National Security Systems
- Improved visibility into National Security System assets
- Consistent incident reporting
- Secure collaboration across organizations and security domains
- Machine-readable policy and compliance guidance
- Better coordination between agencies, CNSS, NSA, and shared service providers
- Greater accountability for cybersecurity outcomes

Rather than prescribing specific technologies, NSPM-12 asks agencies to establish an architectural and operational approach capable of supporting these objectives.

The Opportunity Beyond Compliance

Many federal initiatives begin as compliance exercises. The most successful become modernization initiatives.

NSPM-12 creates an opportunity to strengthen not only cybersecurity posture but also the way agencies manage, govern, and use mission data.

Organizations that take a strategic approach can simultaneously improve:

- Zero Trust maturity
- Cross-domain collaboration
- Data governance
- AI readiness
- Operational resilience
- Cyber resilience
- Mission agility

Instead of creating another isolated compliance project, agencies can use NSPM-12 as a catalyst for building a modern data foundation that supports today's missions while preparing for tomorrow's.

Turning Policy Into Action

Developing an NSPM-12 strategy starts with understanding where critical data resides, how it is governed, who has access, and whether current infrastructure can support evolving security requirements.

A practical roadmap should address questions such as:

- Where does mission-critical data reside today?
- Can data be securely accessed without unnecessary duplication?
- Are policies consistently enforced across security domains?
- Do we have visibility into National Security System assets?
- How will Zero Trust principles be applied to data?
- Is our infrastructure prepared to support AI-enabled missions while maintaining security and governance?

These planning activities often identify opportunities to modernize existing environments while maximizing prior investments.

A Joint Approach

Hitachi Federal and Denodo believe NSPM-12 is fundamentally an architecture challenge, not simply a compliance exercise.

Success requires multiple capabilities working together.

Hitachi Federal helps agencies establish a trusted, resilient data foundation capable of supporting mission-critical workloads, cyber resilience, high availability, and AI-ready infrastructure.

Denodo enables secure, policy-driven access to distributed data through logical data virtualization, allowing agencies to improve governance and collaboration without requiring unnecessary data movement.

Together, these complementary capabilities help agencies create an environment where data remains secure, governed, accessible, and ready to support mission execution across security domains.

NSPM-12 and Zero Trust

Zero Trust is built on the principle of "never trust, always verify."

NSPM-12 extends that philosophy by emphasizing governance, accountability, policy enforcement, and secure collaboration across National Security Systems.

Together, they reinforce a common objective:

- Verify access.
- Protect sensitive data.
- Govern information consistently.
- Reduce unnecessary duplication.
- Improve visibility.
- Enable mission execution with confidence.

By treating data as a strategic asset rather than isolated information silos, agencies can strengthen both Zero Trust initiatives and long-term cybersecurity resilience.

Getting Started

The first step toward NSPM-12 readiness isn't deploying new technology.

It's developing a strategy.

Federal organizations should begin by:

- Assessing current National Security System environments
- Understanding existing governance processes
- Identifying visibility and data-sharing gaps
- Aligning Zero Trust initiatives with NSPM-12 objectives
- Building a phased roadmap that leverages existing investments

Organizations that begin planning today will be better positioned to meet evolving CNSS guidance while enabling future modernization initiatives.

Hitachi Federal

Corporate Headquarters
11950 Democracy Drive, Suite 200
Reston, VA 20190 USA
hitachifederal.com

HF-PAL-EB-NSPM12-DenodoHitachi-28Jul26-A