Securing Smart Solutions: A Cyber Zero Trust Environment

As Smart Solutions proliferate Federal medical logistics centers, depots, airfields, and warehouses, the need to focus on cybersecurity is essential for mission readiness.

Recent Federal mandates and legislation have made implementing a Zero Trust approach crucial for securing smart supply chain solutions in Federal agencies. With technology fueling supply chain performance, the combination of technology, systems, and processes working together in perfect harmony is key to help optimize supply chain functions. What steps can Federal agencies take to integrate Zero Trust into their Smart Solutions?

What is Zero Trust?

Zero Trust is a holistic approach to enterprise information security, treating all identities, devices, networks, and data as untrusted. Least privilege access is granted to users, and proactive measures are taken to prevent worst-case scenarios, to include rigorous authentication, authorization, and verification of a user's identity. Continuous monitoring ensures visibility and baseline activity across all Zero Trust security pillars.

Implementing Zero Trust in Federal Agencies

A thorough Smart Solution with Zero Trust protocols built into the platform is critical – and without compromise. To truly secure the digital experience of Smart Solutions, Federal agencies need to continuously verify and authenticate users' identities, as well as ensure their devices are compliant before granting access. Visibility, analytics, and automation need to be applied continually and comprehensively.

A successful Zero Trust security architecture requires that people, processes, and technology requirements are captured in both strategy and the operational ecosystem. Having a thorough transformation framework in place will not only help streamline the process, but also help ensure it is effective and delivers successful outcomes.

1 **Planning and Prioritization:** Integrating the RMF Zero Trust framework at the early implementation stage allows agencies to improve threat detection, minimize data loss, lower risk, enforce security policies, and maintain public trust

2 **Visioning & Foundation:** Establishing a collaborative and security-conscious vision across the organization, focusing on mission readiness and security

3 **Deployment & Activation:** Putting the right capabilities in place and appropriately releasing the updates to specific stakeholders, ensuring strong data governance, deploying a multicloud strategy, establishing accountability, and fostering a cybersecurity mindset

4 **Change Management:** Guiding the organization, people, and customer journeys, ensuring effective communication and stakeholder engagement

5 **Value Realization & Sustainment:** Identifying key results, value drivers, and key performance indicators to track value, addressing potential roadblocks

6 **Governance:** Setting guardrails for decision-making, managing risk, and ensuring sound governance and internal controls.

How KPMG Can Help

KPMG Smart Solutions are integrated, intelligent, and continuously monitored AI-enabled solutions set to help optimize supply chain functions.

KPMG integrates the Federal Zero Trust RMF from the initial phases of engineering and design, helping ensure security at all levels.

KPMG has worked with Federal government agencies for more than a century. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer supply chain, cyber, and Zero Trust methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter. In addition, KPMG has significant experience implementing supply chain and cyber solutions in both the private and public sectors and can bring those experiences to every government client.

Learn more about KPMG Supply Chain and our Smart Solutions at visit.kpmg.us/fedsupplychain and our Cyber and Zero Trust Solutions at read.kpmg.us/modgov.

Contact us

Meghan Hendery
Principal
KPMG LLP
E: mhendery@kpmg.com

Ishan Kaul
Principal
KPMG LLP
E: ikaul@kpmg.com

Tony Hubbard
Principal,
KPMG LLP
E: thubbard@kpmg.com

Arthur J. Pasagian
Managing Director
KPMG LLP
E: apasagian@kpmg.com

Tyler Carlin
Director,
KPMG LLP
E: tcarlin@kpmg.com

Brian Marshall
Director,
KPMG LLP
E: robertmarshall@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.