Building Cyber Supply Chain Risk Management (C-SCRM) for the U.S. Department of the Interior

The Department of the Interior had to meet Executive Order 14028 across a large network of hardware, software, and service vendors without real-time risk visibility. InterSec, with a product partner, built a C-SCRM program that made supply-chain risk a routine function rather than a special project.

CLIENT	PROFILE	STATUS
U.S. Department of the Interior	Federal lands and resources; large multi-bureau vendor network	In progress

EO 14028
Fully met across the program

SBOM + HBOM
Component authenticity verified

Real-time
Vendor risk monitoring and alerts

NIST SR
800-53 controls for inheritance

DRIVERS	SCOPE	CAPABILITY	ADOPTION
EO 14028, OMB M-22-18	Multi-bureau vendor network	SBOM and HBOM analysis	Training and office hours

THE CHALLENGE

The Department had to comply with Executive Order 14028 while managing a large, varied supplier network, and it lacked a centralized way to identify suspect hardware or software in real time. That gap exposed it to operational disruption and compliance risk. The supply chain was complex and hard to authenticate component by component, visibility was fragmented with no central data, and the compliance stakes were high.

THE APPROACH

InterSec built a C-SCRM program designed to fit into daily operations, so staff could detect and mitigate supply-chain risk as a routine function rather than a one-off project. Adoption was treated as seriously as technology: the team developed user guides for administrators and everyday users, delivered ongoing training across multiple bureaus, and held regular office hours. A targeted framework established repeatable processes supported by integrated tools and dashboards.

> **Supply-chain risk is a program you sustain, not a scan you run once.**

THE SOLUTION IN PRACTICE

InterSec introduced secure data-collection pathways, automated software and hardware bill-of-materials reviews, and coordinated intelligence sharing, giving the Department immediate insight and faster response. Working with a product partner, the program delivered vendor-profile aggregation, SBOM and HBOM analysis aligned with OMB M-22-18, real-time risk monitoring with alerts, secure cross-stakeholder sharing, clear visualization, and multi-group access tuned to different data needs.

RESULTS & IMPACT

- ✓ NIST SP 800-53 SR common controls were documented for consistent inheritance, supporting FISMA and FedRAMP.
- ✓ The program fully met the Executive Order 14028 and OMB M-22-18 directives.
- ✓ Cyber supply chain risks were identified and addressed across the vendor network.
- ✓ Real-time monitoring let the Department address risks early.

KEY TAKEAWAYS

Supply-chain risk management has to live in daily operations.
A program staff treat as routine catches more than one run as a special project.

Adoption is a deliverable, not an afterthought.
User guides, training across bureaus, and office hours make a federal program stick at scale.

SBOM and HBOM analysis turns vendor trust into evidence.
Confirming components are genuine is the difference between assuming a supply chain is clean and proving it.

Document common controls for inheritance.
Capturing the NIST 800-53 SR controls once lets many system owners inherit them.

CAPABILITIES DEMONSTRATED

C-SCRM Framework and Implementation | SBOM and HBOM Analysis | Real-Time Vendor Risk Monitoring | FISMA and FedRAMP Alignment | Stakeholder Training and Adoption

Meeting EO 14028 across a sprawling vendor network takes more than a tool.
InterSec builds C-SCRM capabilities for federal organizations and helps them stick.

Let's talk →