Cybersecurity Supply Chain Risk Management

Reducing supplier risk for the Department of Energy

C-SCRM Program Overview

C-SCRM

CYBERSECURITY-SUPPLY CHAIN RISK MANAGEMENT

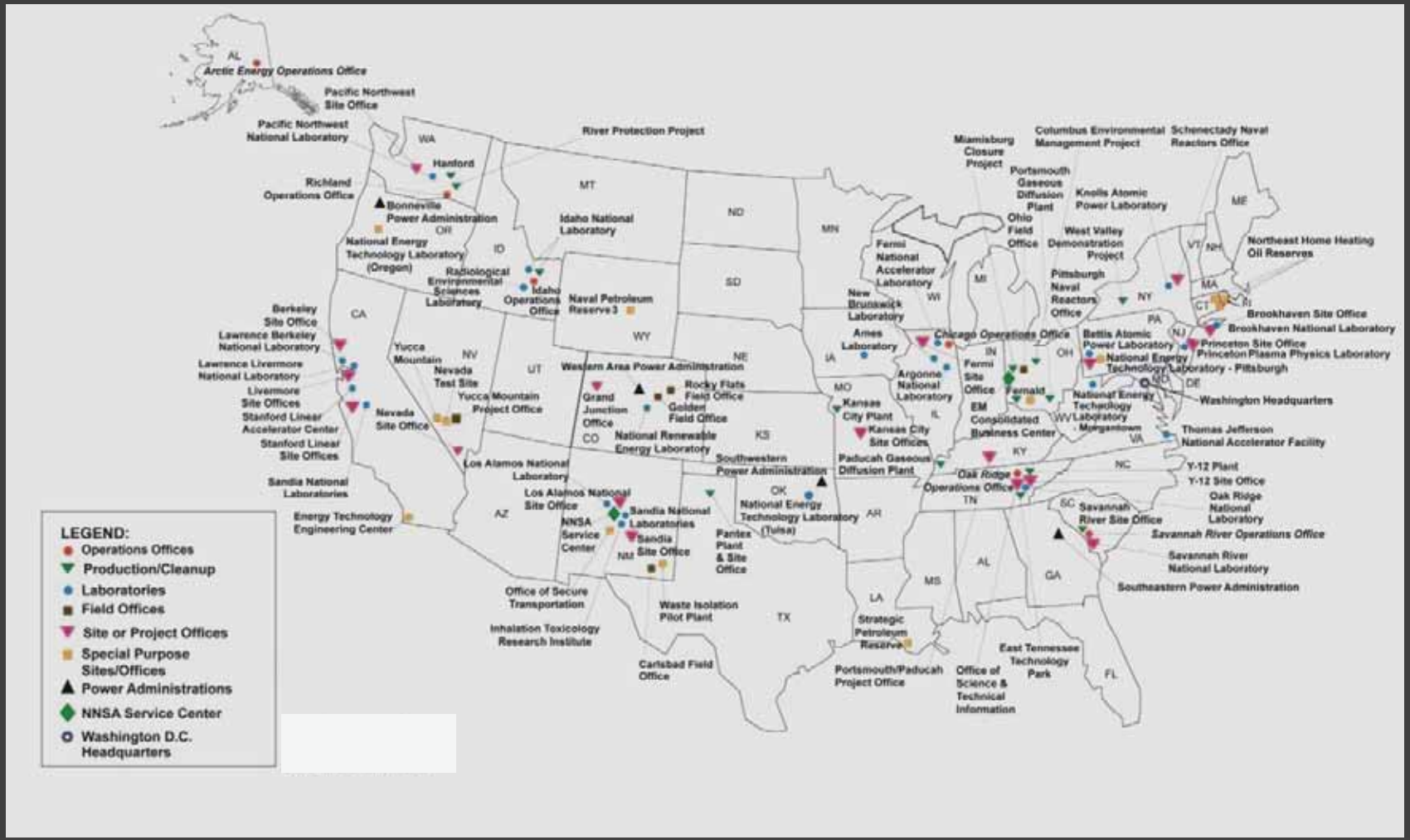
Goals of the DOE OCIO C-SCRM Program

Enable leaders to make risk-informed supplier decisions

Reduce supplier risk throughout the entire supplier lifecycle

Meet and exceed Federal C-SCRM requirements

Department of Energy (DOE) is a diverse and de-centralized environment of **50+ federated entities**, which makes C-SCRM not only unique but very challenging



The DOE compliance and regulatory environment adds further complexity

Office of Management & Budget

Executive Orders

Dept. of Homeland Security

NERC CIP-13

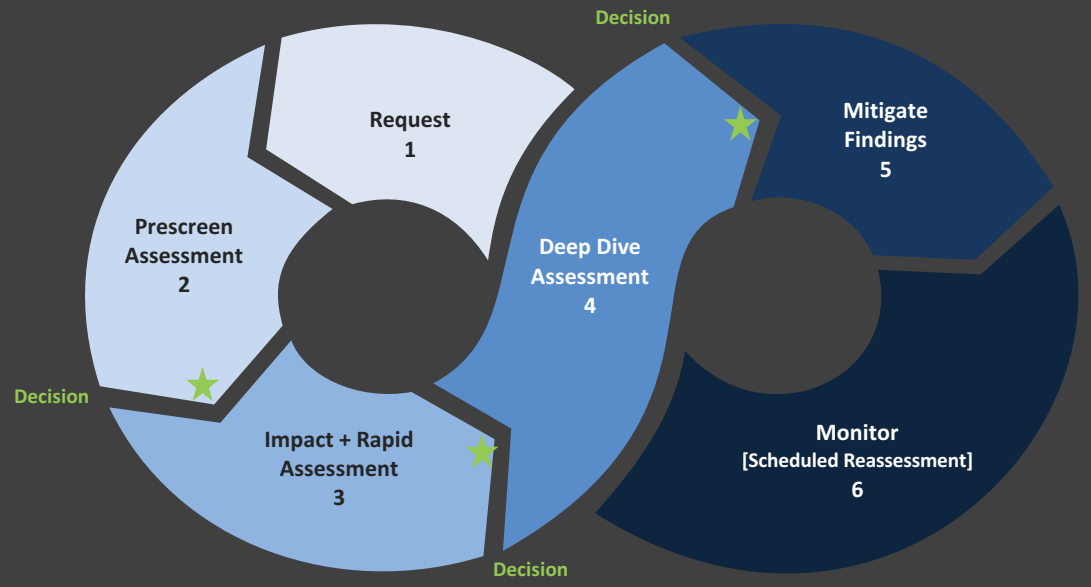
Cybersecurity and C-SCRM Standards

Risk-Based Approach where the greater the risk the greater the diligence conducted

Enablement Approach

- Governance
- Processes
- Technology
- Change Management
- Operations

C-SCRM Process



Risk Lenses

- Cybersecurity
- Foreign Interest
- Resilience
- Compliance
- Federal Utilization

It has been a constant evolution since Aug 2019 to get to where we are today

C-SCRM 1.0

- ✓ Rapid Assessments conducted using four open-source risk lenses
- ✓ Deep dives utilized NIST 800-53 as the baseline security controls
- ✓ Limited automation and email-based communications with customers and suppliers

Aug 2019 - March 2020

C-SCRM 2.0

- ✓ Introduced Pre-screen assessments
- ✓ Enhanced Rapid Assessment
- ✓ Incorporated risk tolerance
- ✓ Established open-source software assessments
- ✓ Implemented external Vendor Portal
- ✓ Became an RMF common controls provider

March 2020 – Aug 2023

C-SCRM 3.0

- ✓ Automated Pre-screen assessments
- ✓ Significantly advanced Rapid Assessment methodologies to incorporate supplier and product
- ✓ Enhanced technology for user experience, increased efficiency for both customers and assessers
- ✓ Added new data elements and risk lenses
- ✓ Deep dives utilize NIST 800-161 V1 to incorporate more specific C-SCRM security controls
- ❑ Further integration with RMF

Aug 2023 - Current

C-SCRM is powered by leading data providers and a robust technology platform

Data Providers

Business Relationship and Economic Threat Analysis (BRETA)

Consolidates 10+ open source, subscription and EY proprietary datasets on 28M+ companies to identify upstream and downstream supplier relationships across 6 risk dimensions and 40 criteria

Publicly Available Repositories

Incorporates publicly available data sources including NIST and CISA vulnerability data, and supplier and product utilization across the federal government and specific agencies

Supplier Data Ecosystem

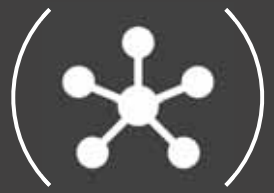
Incorporating additional data sources into C-SCRM assessments to support foreign influence, detailed relationship analysis, and software evaluation (e.g., open source and SBOM evaluations)

Governance, Risk, and Compliance (GRC) Platform

ServiceNow FedRAMP High TPRM

Third Party Risk Management (TPRM) module configured to automate the end-to-end C-SCRM process, centralize risk information (hub), and promote transparency for entities to view their assessments, supplier portal for suppliers to respond to questionnaires, and to enable assessors to provide standardized, objective assessments

Enable leaders to make risk informed procurement decisions, reduce risk and meet Federal requirements with the DOE C-SCRM program



Holistic

End-to-end C-SCRM Program aligned to industry best practice while meeting federal requirements

Assessments: Risk based assessments capable of assessing supplier, product, software or service across 5 risk lenses and 50+ criteria

Data Sources: Utilize curated open source, subscription and gov't data sources to support assessments across 5 risk lenses

Technology: Tailored GRC technology aligned to Federal C-SCRM processes and requirements

Audit Ready: Process aligned to 10 industry frameworks. Supported entity to meet FISMA level 5 C-SCRM maturity

Scalable

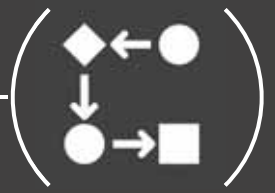
Able to meet the needs of a 'hyper-federated' enterprise while tailoring to unique organizational requirements

Enterprise Scale: Supporting 53+ DOE Entities with diverse risk profiles

Customizable: Can individually account for an organizations risk preference and C-SCRM lens weightings

Common data elements: Ability to share assessment data across large user base

Data Set: Completed over ~7K supplier assessments which can be leveraged to rapidly support a C-SCRM program build



Agile

Able to rapidly adapt to the continuously changing C-SCRM risk landscape and federal requirements

Enhancements: Completed 100+ enhancements to improve processes and technologies

SBOM & SSDF: Researched and introduced net new technologies to enable intake and assessment of SBOM's and Secure Software Development Attestations

Rapid Deployment: 2-week rapid entity onboarding capability focusing on process and technology training and service customization

Operation Reviews: Periodic entity reviews of assessments outcomes, metrics, and feedback to continuously improve program

C-SCRM TOP 3….CHALLENGES AND LESSONS LEARNED

Number 3…Top Challenge and Lesson Learned about C-SCRM

Challenge:

Letting a C-SCRM program go stale

Lesson Learned:

- Build a strong foundation of governance and process
- Keep scalability in mind
- Enhance based upon user experience and new capabilities
- Have a robust change management process

Number 2…Top Challenge and Lesson Learned about C-SCRM

Challenge:

Balancing technology, process, and people

Lesson Learned:

- Find your organizational champion (s)
- Collaborate…collaborate…collaborate
- C-SCRM can change how people procure and use ICT…train and manage change closely

Number 1…Top Challenge and Lesson Learned about C-SCRM

Challenge:

Excessive amount of guidance, tools, data and suppliers

Lesson Learned:

- Develop your North Star…what do you want your C-SCRM program to be
- Stay current…constantly evolving environment

QUESTIONS

Contacts

Contacts:

- Federal Program Lead: Shannon Hughes, Shannon.Hughes@hq.doe.gov

"The C-SCRM program is an integral component of our cybersecurity risk management program and provides capabilities that would be difficult to staff within our organization. The information provided greatly assists us in making risk-based decisions to enhance the security of our mission to safely provide reliable, cost-based hydropower and transmission to our customers and the communities we serve."

"The C-SCRM program provides a great service and value, enabling sites to focus limited resources on other priorities. Leveraging the wide range of risk information that the C-SCRM program provides allows us to make risk-informed decisions that continue to enable and improve the security of our mission."