White Paper
for the
Energy Facilities Contractors Group (EFCOG)

Review of Supply Chain Risk Management at Energy Federal Contractor Organizations

Summary of Observations, Lessons Learned, Processes, Best Practices, and Recommendations in Supply Chain Risk Management

by the

Energy Facility Contractors Group
Supply Chain Task Group, Supply Chain Risk Management Subgroup

Co-Chairs: **Amy Lientz, Idaho National Laboratory (primary author)**
Jason Eaton, Consolidated Nuclear Security, LLC

E-SG-SCRM-2021-7, Revision 0

July 2021

Principal Authors/Reviewers of this Document from Supply Chain Risk Management Subgroup

Author:

- **Amy Lientz,** Director Supply Chain Energy Programs, Idaho National Laboratory, and Co-Chair SCRM Subgroup

Contributing Author:

- **Jason Eaton**, Senior Director, Supply Chain Management, Consolidated Nuclear Security, LLC, and Co-Chair SCRM Subgroup

Reviewers and Contribution:

- Amber Romero, Sandia National Laboratory
- Matrice Endres, Sandia National Laboratory
- Steven Pierson, Kansas City National Security Campus
- Barbara Siciliano, Idaho National Laboratory
- Mike Drake, Idaho National Laboratory
- Spencer Daw, Idaho National Laboratory
- Jane Strong, Idaho National Laboratory
- John Robinson, Hanford Site
- Janette Robinson, Savannah River Site
- Kristi Haataja, Lawrence Livermore National Laboratory
- Gary Wolski, Curtiss-Wright
- Laura Valdez, Consolidated Nuclear Security, LLC

EXECUTIVE SUMMARY

The COVID-19 pandemic and other disruptions have influenced supply chains to become more complex, volatile, and fragile, thus creating notable challenges in delivery and performance where security vulnerabilities have taken center stage. This supply chain volatility is expected to be an ongoing concern for organizations in the future with a wide array of environmental forces acting on the global supply chain. Managing the critical business practice of supply chain risk requires increasing all entities awareness as the supply chain evolves within the U.S. Department of Energy (DOE) Complex. This white paper details the benchmarking of Supply Chain Risk Management (SCRM) processes for DOE contractors and select vendors. The SCRM Task Group led these efforts from January 2020 to June 2020.

Many of the challenges can be solved without adding new DOE requirements or policies, but through the implementation of best practices and considering recommendations for improvements. The key observations summarized below represent considerations from DOE contractor organizations, each observation leads to further detail later in the report.

Table 1. SCRM Key Observations in the DOE Contractor Community.

SCRM Maturity	The more mature SCRM programs exist within the Department of Defense (DoD) from a decade long practice of implementation. Within DOE, only a few DOE contractor organizations show mid-stage maturity in SCRM . This includes the following National Nuclear Security Administration (NNSA) Sites: Kansas City National Security Campus (KSNSC) and Sandia National Laboratory (SNL). SCRM at other DOE contractor sites reveal low maturity and several have not yet considered developing a SCRM process or program.
Supply Chain Flow-down Requirements	Representative contractor organizations shared concerns about the potential of adding more supply chain flow-down requirements without commensurate deletions and reductions of other requirements. Some observers shared the increasing difficulty vendors experience in trying to meet flow-down requirements to bid on work. Small businesses in particular experience the most challenge meeting contractor requirements.
Organizational Structure and Commitment to SCRM	While all contractor organizations exhibit moderate to high levels of concern regarding supply chain risk, the NNSA laboratories showed more maturity with a formalized approach to addressing SCRM with an organization separate from the procurement organization, dedicated staff, approved analytical risk tools, guidelines, training programs, and dedicated resources.
Quality	High-end and mission critical products, such as nuclear grade materials, industrial components, software, hardware, etc., require strict quality control, reviews, and assessments. Some contractors have integrated their quality programs with SCRM. However, this model does not work for every organization and this decision should be left up to the contractor as to what makes the most sense for their operations.

Standardization and Clarity of Requirements	While flexibility is important in the adoption of a SCRM program that makes sense to the contractor organization, there are examples where standardization should be reviewed further: flow-down requirements, risk assessments, definitions, supplier scorecards, and SCRM best practices. Additionally, sites are seeking clarity on existing regulations tied to SCRM.
SCRM Analytical Tools	Easier access to cloud-based data analysis tools is needed to perform detailed risk reviews of vendors. Often, FedRAMP or internal contract clauses prevent access to necessary tools, which in turn makes for a lengthy and costly process to receive certification.
Training and Education	More training and education internal to the contractor on SCRM is essential so there is understanding of the need and purpose, concerns can be identified, and solutions can be addressed. Similar training programs should be considered to vendors and suppliers of the contracting organization and the ability to share this information with sub-tiers, as necessary.
Collaboration and Sharing	Better and more well-defined communication from buyer to vendor is important to ensure a clear understanding of flow-down requirements and performance risk areas, as well as where a vendor may need additional buyer information or assistance. Many companies have recognized that stronger relationships are needed, as well as ways to address vendor-managed risk and improve efficiency between the buyer and the vendor. A strong collaborative process with well-managed information sharing is critical for success. Contractors have much to gain from learning from other contractors on such things as training, software tools, supplier performance and concerns, internal work processes, etc.

Review of Supply Chain Risk Management at Energy Federal Contractor Organizations

Table of Contents

1. INTRODUCTION

This document, which describes the efforts of the Supply Chain Risk Management (SCRM) subgroup, as described below, is endorsed by the Energy Facilities Contractors Group (EFCOG). The purpose of this effort is intended for use by U.S. Department of Energy (DOE) contractors considering implementing SCRM processes or standing up a similar program. To assist organizations in addressing growing concerns and risks in supply chain processes, a benchmark of existing programs within the DOE Complex was conducted for both contractors and select vendors of contractors. Additionally, information was reviewed from other existing SCRM programs outside of the DOE environment. This report summarizes the results of these efforts in the following categories:

- DOE Contractor Survey Results on SCRM Implementation
- DOE Contractor Supplier SCRM Considerations
- Other DOE and non-DOE SCRM Observations
- A Summary of Recommendations for SCRM Programs.

1.1 SCRM Subgroup Charter and Team Members

In December 2020, the SCRM subgroup was chartered, which was chaired by Darrell Graddy of Leidos. The charter of this subgroup is as follows:

SCRM Subgroup Charter

Benchmark a diverse set of DOE contractor organizations as to how contractors are addressing evolving SCRM concerns and policies.

The Task Group Team

Organization	Team Members
Idaho National Laboratory	Amy Lientz – Co-Chair Barbara Siciliano, Mike Drake, Spencer Daw Jane Strong (project administrator)
Consolidated Nuclear Security, Y-12 National Security Complex and Pantex Plant	Jason Eaton – Co-Chair Laura Valdez
Sandia National Laboratory	Amber Romero Matrice Endres
Kansas City National Security Campus	Steven Pierson
Hanford	John Robinson
Savanah River Site	Janette Robinson
Lawrence Livermore National Laboratory	Kristi Haataja
DOE Vendors: Curtiss-Wright	Gary Wolski

1.2 Supply Chain Definitions and Considerations

Supply chain requirements in managing risk is not yet fully institutionalized within DOE; therefore, a common definition used among the contractors through the EFCOG organization was important. The following are the definitions used to support the efforts of data collection from the contractors and the vendors.

Supply Chain (as defined by a prior EFCOG Supply Chain Task Group): The supply chain is the over-arching system of interrelated processes for the planning, procurement, receipt, and storage of items and services that apply to DOE Complex sites. This includes baseline planning, budgeting, specification development, procurement evaluations, the acquisition of services, material control, vendor evaluations, quality control inspections, material storage and disposition, and contract closeout. Importantly, it also includes the coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers.

SCRM (as defined by DOE O 452.4C): The systematic identification, assessment, quantification, and mitigation of potential supply chain disruptions. ***NOTE: For purposes of this benchmarking effort, the definition was not limited to national security or cybersecurity concerns.***

Policy Considerations. Over the last five years, there has been increasing policy level attention from the current administration, as well as the prior administration, on strengthening the U.S. supply chain. As a result, many policies and directives have been developed for both federal offices and their contractors. These policies result in implications that require consideration. While not an exhaustive list, Barbara Siciliano, SCRM Director, compiled a list of the most recent policy considerations for DOE contractors:

- Executive Order (EO) 13920, "Securing the U.S. Bulk Power System," 2020 (currently on-hold)
- "The Domestic Preference Laws"- this includes the "Buy American Act", 2019 ; the "Trade Agreements Act" 1979; and "The Berry Amendment", 1994.
- Intelligence Committee Directive (ICD) 731, "SCRM Standards," 2019
- Title II of the Secure Technology Act, "The Federal Acquisition Supply Chain Security Act of 2018," 2018
- EO 13806, "Assessing, Strengthening Supply Chain Resiliency of the U.S.," 2017
- Committee on National Security Systems Directive (CNSSD) 505, "SCRM Directive for National Security Systems (NSS)," 2017
- Committee on National Security Systems Policy (CNSSP) No. 22, "Cyber Security Risk Management Policy," 2016
- National Institute of Standards and Technology (NIST) 800-161, "SCRM Practices for Federal Information Systems and Organizations," 2015
- "Cyber Maturity Model Certification v 1.0," released January 1, 2020
- EO 14028, "Improving the Nation's Cybersecurity," May 12, 2021
- EO 14017, "America's Supply Chains," February 24, 2021
- "American Supply Chain Reports," June 8, 2021.

2. DATA COLLECTION

The SCRM Task Group collected data using the following processes as described briefly below:

- Presentations and Guest Discussions:

- The Task Group met every three to four weeks and often invited a key SCRM leader to present information on their organizations' SCRM program or discuss a topic or subject of interest related to SCRM. Information was collected from these discussions to inform the final benchmarking efforts and feed recommendations. The following people discussed their organizations and other topics through the Task Group meetings: Amber Romero (SNL); Steven Pierson and Tim Schalm (KSNSC); Jason Eaton (DoD SCRM Program); Amy Lientz (Air Force SCRM Recommendations); Gary Wolski (A vendor perspective from Curtiss-Wright).

- Interviews or Follow-On Discussions:
  - To obtain clarification on information either outlined in the survey or to obtain additional perspective in certain areas of interest, phone calls were scheduled with experts. One interview was conducted on SCRM with the Electric Power Research Institute (EPRI).
- Surveys:
  - Two survey formats were developed by the Task Group one for contractor organizations and another for vendor organizations:
  - A request to 25 contractor organizations was sent on May 1, 2021, which included National Nuclear Security Administration (NNSA) Laboratories, Environmental Management Contractors, and non-NNSA National Laboratories. The survey sent to contractors is presented in Appendix A.
  - There was a 56% response rate (14 surveys returned):
    - 46% non-NNSA laboratories
    - 50% Environmental Management (EM) sites
    - 66% NNSA sites.

3. RESULTS OF DATA COLLECTION

Results of the surveys and presentations are discussed further in the sections that follow.

3.1 Survey Results

The survey results were collected between May 1 and June 1, 2021. The survey form is presented in Appendix A. Information was collected by both the prime contractors for DOE and key vendors for the prime contractors.

3.1.1 Vendor Insight on SCRM

- Large business vendors to DOE contractors are increasingly concerned.
- For vendors that participate in the Defense, Aerospace, and Medical industries, notable efforts in developing supplier risk assessments and mitigation plans are available. Businesses that participate in the power markets are just beginning similar activities.
- Most businesses have not seen flow-downs from the prime contracts specific to SCRM.
- Defense and Aerospace-related businesses have participated in customer-driven risk assessments for several years now. These assessments are typically referred to as Program Readiness Reviews or Rate Readiness Reviews, both of which evaluate a supplier's ability to perform, including Supply Chain Management practices.
- There are larger suppliers that provide products and services to Aerospace/Defense contractors—including Lockheed Martin, Boeing, and Parker—who have all benchmarked other organizations in SCRM practices. They all found that larger and longer-term defense contractors/suppliers have

mature SCRM programs that operate similarly. Each SCRM program required intimate engagement with key suppliers.

- Key products of concern include electronics, specifically semiconductors. The ripple effect has impacted the availability of plastic resins used to manufacture circuit boards. Similar challenges are coming to light with specialty alloys that are utilized in electrical components.
- A recommendation to DOE and to DOE contractors would be to standardize guidelines, as well as terms and conditions, for SCRM. Also, large suppliers should have standard assessment tools to evaluate their supply base and rigorous action plans to mitigate. Supplier visibility is becoming more prevalent (i.e., visibility into suppliers' work-in-process, sub-supplier deliveries, commitment dates, etc.).
- The biggest need to starting or improving a vendor SCRM program is in its access to funding and talent resources and approved software tools to assist in risk assessments.
- Small suppliers have generally not implemented a SCRM program. There are those that are learning, preparing, and considering formalization of a SCRM program, but lack the resources or the talent to implement a program.

3.1.2 Contractor Results

Results of the Survey sent to DOE prime contractors are included in Appendix B. Key recommendations are also included in Appendix B and discussed in Section 4.

3.2 Observations from Sites with Mature SCRM Programs

There were three presentations made to the task force that included discussions of existing SCRM programs, lessons learned, and best practices. The three presentations came from the following organizations:

- SNL: Amber Romero
- KSNSC: Tim Schalm
- DoD: Jason Eaton

In assessing each presentation, similar concerns and opportunities were noted. A few key observations include:

- The use of metrics and inspections as methods for SCRM is in its infancy and is still maturing. The NNSA laboratories are further ahead in implementing SCRM programs. DoD has had a long-standing SCRM program. Other DOE organizations are further behind in implementing SCRM programs.
- The ability to access software tools to assist with risk analysis is important to a SCRM program.
- Cross-cutting education among internal stakeholders of purpose and intent of SCRM is critical.
- The ability to share supplier information would provide an excellent benefit across all service areas.
- A consistent approach to contractual flow-downs should be addressed. Considerations of impacts to implement flow-downs to sub-tiers need to be considered.
- Processes and guidelines to assess risk should be graded depending on what is being assessed.

These and other observations are broken into three categories for further discussion: (1) Organizational Considerations; (2) Information Technology (IT) Systems; and (3) Cybersecurity.

1. **Organizational Considerations (includes Quality, Policies, and Logistics)** – These risks encompass all aspects of supplier performance. Examples include (but are not limited to) items such as financial, manufacturability, affordability, configuration management, capacity, quality controls,

lower level sub-tiers, critical and raw material strategies, and general Business Management. Supply Chain Risk was a leading concern in assessing the quality of suppliers at KCNSC, SNL, and DoD.

Takeaway – Key insights in assessing risk as it relates to the organization and organization processes and policies, including quality, are as follows:

- There are risks within the supplier's business that result from the inability to meet the expectations of government contractual flow-down requirements, which are much more stringent than commercial sales. Lower sub-tier suppliers and small business suppliers have the most challenges in meeting new flow-down requirements related to SCRM.
- Current DoD/DOE Supply Chain Management requirements instituted by the Defense Contract Management Agency (DCMA) and the NNSA Production Office (NPO) are inconsistent and leave significant room for interpretation by individuals responsible for oversight. Interpretations stemming from personnel turnover, as well as cause and corrective action requirements, often result in flow-down changes that prevent or eliminate a standard, consistent approach.
- Supply chain risk assessments are often performed on policy/procedure compliance issues rather than the overall aspects of the supplier's performance capabilities. One example that was given stated that when an escape occurs, localized procedure or policy changes result in additional requirements vs. reviewing, clarifying, and restating the process for mitigation. Caution should be given to quick reaction policy/procedure changes based on human error or process gaps. This compiling of requirements creates significant non-value-added work and rarely addresses the root cause of the risk. Mistake-proofing process updates within the existing policy or procedure would likely provide a much greater solution.
- SCRM organizational structure affects quality and other processes. Different areas of responsibility for the same processes are assigned to different organizations. This becomes problematic when each organization using its own priorities develops unique "standard work" definitions, thereby causing processes to become fragmented as a whole. This also makes it difficult to find who the process owner is, as well as how to control the implementation of the changes that impact both up- and down-stream processes. To manage risk, "standard work" should be used wherever possible, regardless of organizational owner.
- Businesses and suppliers must be more systemically integrated enabling automatic transmission of data. Today, transactions typically used for lower level risk materials are subject to the same restrictions as the most complex versions of data transfers. Together cybersecurity and the Supply Chain Management teams must identify opportunities to enable low-risk integration structures or a graded approach to complexity or concern for products or services. Additionally, while focus is given on the quality levels for inspection purposes, finding such issues during the inspections process only means that a failure occurred upstream. This same effort should be given to understanding where risk areas exist in the manufacturing process and eliminating failure there.
- Consider a SCRM program that is cradle-to-grave, which starts with procuring, logistics of transportation and delivery, installation and maintenance, and disposal. Each phase of the supply process could impose a risk or vulnerability. Most SCRM programs focus on the procurement process, but maturing programs are considering the lifecycle of the supply chain.
- Supply Chain Management teams do not have adequate access to today's SCRM tools that would enable subcontract managers to perform a comprehensive capability assessment and to view past performance indicators prior to contract award. Instead, time is spent collecting documentation to "check the box," which is then used to signal "qualified or low risk." The act of truly understanding a supplier's weakness has become reactionary when a quality or vulnerability escape occurs—such as in the counterfeit parts. With proper upfront assessments, a SCRM program would be able to take proactive measures to avoid potential risks. In addition, advance

SCRM tools are beginning to develop predictive modeling capabilities that will detect anomalies in well recognized patterns and alert action to mitigate potential risk events.

2. **IT Systems** – Having systems with the ability to identify red flags and trends, find mistake-proof inputs, establish pre-set contract rules based on established criteria, and be interactive across multiple functions requires IT-integrated service capabilities. DoD systems appear to be more integrated than DOE systems; however, the technology for both is significantly less than that of most major commercial businesses today. The typical response for the lack of superior IT systems in the Government Sector is the lack of funding and/or resources, integration capabilities, or cybersecurity concerns. There is a Technology Modernization Fund (TMF) that could potentially fund modernization of IT systems. Many are not aware of this fund. More information can be found at: https://www.gsa.gov/technology/government-it-initiatives/technology-modernization-fund.

   Takeaway – SCRM should utilize integrated, robust supplier assessment tools. The SCRM teams across DOE should play a major role in the early identification and evaluation of IT system strategies that drive process efficiencies, as well as ensure relevant risk information. The following are several insights identified from the more mature programs that were reviewed:

   - Education and awareness of SCRM is important with key members of IT, so it is clear as to what the problem is that SCRM is trying to solve, as well as a better understanding for the need of useful SCRM tools that aid in supplier risk reviews and mitigation plans.
   - There are tools available today that would enable SCRM programs to perform supplier risk assessments. Additionally, there are external systems available that compile current suppler data and business attributes that would aid in risk identification. However, due to lack of funding, resources, knowledge of existence, or cyber vulnerability concerns, these systems are not always made available to the SCRM program. Without the availability of these tools, effective risk mitigation will remain in a reactionary mode.
   - Consider forming a System Change Board. In most cases, the SCRM program is at the mercy of IT, cybersecurity, and/or individual organizations choosing new systems through the network, which ends up impacting the supply chain processes. To break this cycle, consider forming a System Change Board, such as those used for engineering changes. System Change Boards could ensure that every organization has the necessary information to assess the risk or impact of new software or system changes prior to implementation. Without this review, even changes meant to reduce risk for one area often result in elevating risks for another. IT should lead these change boards with sign off from all organizations. This same board could assist in the selection of the most appropriate SCRM tool that would yield organizational integration and data sharing opportunities.

3. **Cybersecurity** – The skill set for cyber risk identification and risk management is very specific and most portions of it reside outside of the SCRM program. SCRM is typically the recipient of cybersecurity risk mitigation strategies, as these risks start and extend from the overall business strategies, and contractual and operational flow-downs.

   Takeaway – The following insights were provided by the organizations that were reviewed on the integration of cybersecurity and SCRM:

   - There is room for improvement to integrate SCRM with cybersecurity reviews on risk. There is balance in managing risk while still delivering an efficient, manageable, timely supply chain of goods and materials.
   - When risk mitigation causes stagnation, other options must be explored, including possible policy changes.

- Consider a graded approach to cybersecurity reviews of the supply chain. Not all constraints would be applicable to all areas; however, sites have taken the less expensive path in making decisions across the board rather than investigating applicability for some of the easily mitigated/low risk constraints.
- Clarifications for some of the constraints would be helpful in determining risk levels. In addition, the SCRM program could potentially help IT or cybersecurity identify solutions that could assist in mitigation.
- Cybersecurity often considers the role of the SCRM program as a compliance-centered effort vs a part of the mitigation process. Early education to the cybersecurity experts of what SCRM is and what SCRM is not is recommended.
- Strong and mature SCRM programs benefit by having integration between the SCRM program and cybersecurity.

4. Recommendations

In summary, here is a list of the recommendations and considerations compiled from presentations, survey input, and interviews as detailed above. As contractors stand up a SCRM program and as DOE considers guidelines for SCRM:

1. Allow the ability to leverage the use of cloud-based big data and analysis tools without lengthy delay associated with the FedRAMP requirement. Continuous monitoring solutions need to be implemented faster. Also, a SCRM Software as a Service (SaaS) solution allows illumination of risk at a sub-tier level where the probability of risk increases.
2. Share information among the DOE contractors:
   a. DOE/NNSA Wide Contractor Past Performance Database (e.g., vendor feedback upon contract closeout).
   b. High-Level Audit Findings.
   c. Lessons Learned from Procurement/Supply Chain.
   d. Centralized supplier clearinghouse that supports SCRM efforts. An example would be what DoD is doing on their Exostar platform for Official Use Only (OUO)/Controlled Unclassified Information (CUI) vendors at all tiers.
   e. Approved supplier list that ties in with the overall commodity strategy that is available across the DOE Complex.
3. Training tools and resources should be made available:
   a. Consider developing SCRM processes to quickly identify, assess, prioritize, and mitigate supply chain risks and train this at all levels of the organization to build awareness.
   b. Counterfeit and cyber-training should be useful regardless of site. Teaching about gray market resellers and how to authenticate is paramount.
   c. General Buyer Training on Quality Assurance (QA) Risk Management Process and Business Risk Management Processes.
   d. Training vendors and suppliers on expectations and how to reduce risk.
4. Provide clear guidance on regulations and requirements:
   a. Clarity is needed so that contractors can more effectively implement and meet customer needs and expectations (e.g., DOE, programmatic, etc.).
   b. Standardize supplier ratings systems with clear explanations of supplier rating systems.
   c. Consider a performance or compliance scorecard.

5. Develop a business-friendly framework for implementing SCRM among the contractors that can also be adopted easily by the vendors. (Note: Focus on the key risk elements that will harm the contractors and enterprise, and share guidance on when to accept risk, how to mitigate, and when to not accept). Customization by site should be allowed to incorporate business/operational requirements to support mission work.
6. Provide insight on specific flow-down terms, such as indemnity and limitation of liability. Note: contract clauses are an increasing challenge. DEAR 970.5244-1 notes that Maintenance and Operations (M&O) contractors cannot accept indemnity on behalf of the federal government, and this has been construed to also apply to Limitations of Liability—a challenge when negotiating Terms and Conditions. Include guidance as to how to include SCRM requirements into contract language.
7. More resources in terms of funding and talent are needed to support effective SCRM programs across the DOE complex.

5. SCRM Task Group Follow-On Considerations

The SCRM Task Group unanimously recognized value in continuing EFCOG SCRM efforts into the next year. The following were recommendations from team members as to areas of focus that would have value in cross-contractor participation:

1. **Review SCRM tools used across the contractor complex.** As awareness of supply chain risks grows among federal agencies, there is a greater need for tools that evaluate the impacts of a supply chain-related cyber event. This can be a difficult activity, especially for those organizations with complex operational environments and supply chains and can be an expensive activity for small contractor organizations that do not have the funds or the talent to support such a tool. The team determined that a working group to assess tools used by DOE contractors that have a more mature SCRM program and tools being considered by other organizations would be a value-add next step of this organization. Further definition of what this would include should be reviewed.
2. **Share resources to educate and train internal employees and vendors in SCRM practices.** As a more common understanding of SCRM permeates the DOE sites, the benefits of common training, informational papers, and other resources will add value to all personnel impacted by SCRM. A working group to look into ways to consolidate this information, identify training resources, and potentially look at opportunities to utilize the DOE Contractor Acquisition University platform to help disseminate the knowledge is essential in arriving at a common set of SCRM practices. The goal would be the identification of the type of resources and the platform where the knowledge could reside.

Appendix A
Supply Chain Survey Sent to U.S. Department of Energy Contractors

ENERGY FACILITY CONTRACTOR ORGANIZATION GROUP (EFCOG) SCRM TASKFORCE

QUESTIONAIRE on SCRM FOR DOE CONTRACTOR ORGANIZATIONS

The purpose of this questionnaire is to assist in benchmarking Supply Chain Risk Management (SCRM) maturity and concepts of DOE/NNSA contractors. It is recommended that this survey is taken by someone in the organization that is responsible for implementing supply chain and/or procurement in your organization. This information will be complied to help assess best practices, maturity of SCRM programs across the DOE contractor organizations, and will be used to inform contractor members to EFCOG with suggestions and recommendations that may be helpful to member organizations. While answers and data may be shared with DOE/NNSA during discussions, all data and comments will be aggregated and data will not tie locations to specific responses or comments unless the responder has provided approval. Not all organizations will be able to answer the questions depending on the maturity of their organization and that is informative as well. Please respond to all questions to the best of your ability and you are welcome to include attachments you would like to share (procedures, presentations that describe your program further, etc.). ***Please complete by May 30th, 2021 and send an attached completed survey in word format to amy.lientz@inl.gov and jason.eaton@cns.doe.gov.***

Thank you for your time, EFCOG Supply Chain Risk Management Taskforce
Co-Chairs: Amy Lientz, INL Supply Chain Director Energy Programs and
Jason Eaton, Senior Director Supply Chain Management, CNS, llc (Pantex/Y-12)

Name: Click or tap here to enter text.
Organization and Title: Click or tap here to enter text.
Contact Information (email and phone number): Click or tap here to enter text.
ORGANIZATIONAL INFORMATION

1. **On a scale of 1 to 5 (with one being least concerned, 5 being most concerned) how concerned is your organization/business unit about supply chain risks?**

1	2	3	4	5
☐	☐	☐	☐	☐

Low Concern High Concern

2. **What level of organizational leadership has been briefed and is aware of SCRM? (select all that apply)**
   - ☐ CEO/COO
   - ☐ Vice President/Business Unit leadership
   - ☐ Sr. Director/Director of Functional Area
   - ☐ Line Management Leadership
   - ☐ Non-Management Leadership/Subject Matter Experts
   - ☐ Not Applicable

3. **Has your organization established an ongoing process of assessing supply chain risk? If "Yes", please describe.** ☐ Yes ☐ No
   Additional Detail Click or tap here to enter text.

4. **Does your org have a formal SCRM department or does each business directorate have separate SCRM responsibilities? If "Formal" please provide position titles and additional details. If decentralized, briefly describe the structure.**
   ☐ Formal SCRM Department ☐ Decentralized
   Position Title(s): Click or tap here to enter text.
   Additional Details: Click or tap here to enter text.

a. **Do you have an SCRM Risk Register which maintains all site wide risks?** ☐ Yes ☐ No
b. **Does it include mitigation plans and/or actions?** ☐ Yes ☐ No
c. **How do you prioritize risk in the supply chain (i.e. what events are considered highest risk to your organization, what are moderate/low)?** Click or tap here to enter text.
d. **Is your SCRM program integrated with existing quality control review processes?**
e. ☐ Yes ☐ No **Please explain:** Click or tap here to enter text.
f. **Do you perform a risk review of documents/information going to suppliers prior to sending out?** ☐ Yes ☐ No
g. **What controls have you implemented to prevent gratuitous information from being sent to suppliers?** Click or tap here to enter text.

SUPPLIER SCRM

5. **Are you periodically collecting risk information from your critical suppliers?** ☐ Yes ☐ No
If yes, please detail out what actions can/do result from adverse information (i.e. corrective actions, removal from Approved Supplier Lists, notices, etc.) Click or tap here to enter text.

6. **What types of tools does your organization use to evaluate suppliers to assess risk? (select all that apply)**
☐ Artificial Intelligence/Machine Learning for supplier risk management
☐ 3rd party solutions using SCRM cloud-based applications for continuous monitoring
☐ 3rd party research and marketplace intelligence tools
☐ Other (Please Detail): Click or tap here to enter text.
Additional Detail on tools: Click or tap here to enter text.
☐ Not Applicable

    a. **What challenges has your site faced in implementing commercially available SCRM tools (i.e. FedRamp certification for commercial suppliers, internal IT requirements, funding, etc.)** Click or tap here to enter text.

7. **What corrective action techniques does your organization use for suppliers if adverse SCRM information is developed during execution?** Click or tap here to enter text.

8. **Do you analyze supplier exposure to risk in the evaluation process and how is it utilized? (select all that apply)**
☐ Go/No-go criteria
☐ Weighted criteria
☐ Unevaluated information
☐ Other: Describe Click or tap here to enter text.
☐ Not Applicable

TRAINING

9. **What type of training related to SCRM does your organization provide? (select all that apply)**
☐ Internal Requestor Training
☐ Internal Quality Training
☐ Internal Procurement Training
☐ Supplier Awareness Training
☐ Suspect/Counterfeit Item Training
☐ Inspection Techniques
☐ Other: Describe Click or tap here to enter text.
☐ Not Applicable

10. **What types of trainings would you find useful that could service multiple sites (i.e. SCRM trainings that do not depend on your implementation)?** Click or tap here to enter text.

CHALLENGES

11. **What do you consider your biggest challenge in decreasing Supply Chain Risk for our suppliers?**
    ☐ Confusing/Conflicting flow-downs
    ☐ Boilerplate terms and conditions that are not tailored for the specific procurement
    ☐ Poorly defined requirements/expectations
    ☐ IT policies/restrictions can't keep up with commercial products (i.e. can't have WiFi/Bluetooth, but almost all rental/lease equipment companies have it in their offerings for loss prevention)
    ☐ Referencing all possible DOE regulations that could apply to a procurement vs. calling out only the specific applicable sections
    ☐ Other Click or tap here to enter text.
    ☐ None

12. **Which DOE/NNSA improvement project would benefit your organization/supply chain the most?**
    ☐ Standardized terms and conditions among sites
    ☐ Centralized supplier clearinghouse (similar to what DoD is doing on their Exostar platform for OUO/CUI vendors at all tiers)
    ☐ Other: Explain Click or tap here to enter text.
    ☐ Not Applicable

13. **What is your organization's biggest need in relation to starting/improving your SCRM efforts?** Click or tap here to enter text.

Page intentionally left blank

Appendix B
EFCOG SCRM Subtask Benchmark Survey Results

May 2021

Survey Notes and Legend

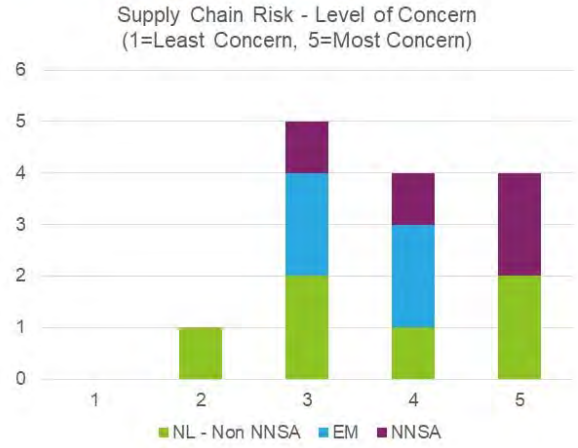
- **Sent 25 surveys out on 5/1/2021 to DOE contractor organizations.**
  56% response rate (14 surveys returned)
  - 46% non-NNSA labs
  - 50% EM sites
  - 66% NNSA sites
- Survey had 13 questions, several with multiple parts

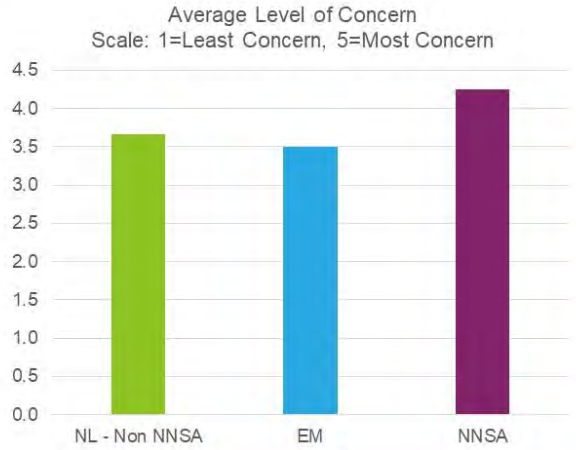
- All graphs use a consistent color codes to identify facility types
  - National Labs – Non NNSA
  - EM
  - NNSA
- For text responses, similar topics that are addressed by multiple respondents appear in **bold and are underlined**.

2

IDAHO NATIONAL LABORATORY

1) On a scale of 1 to 5 (with one being least concerned, 5 being most concerned) how concerned is your organization/business unit about supply chain risks?

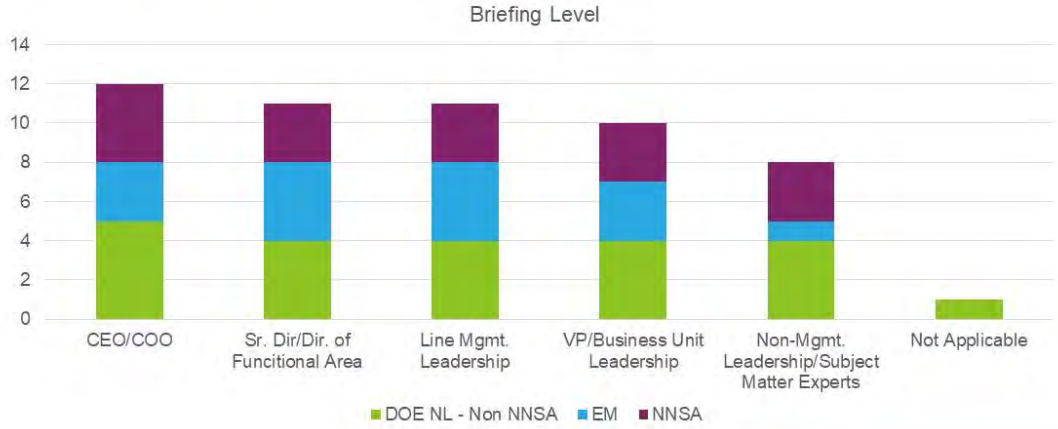




3

IDAHO NATIONAL LABORATORY

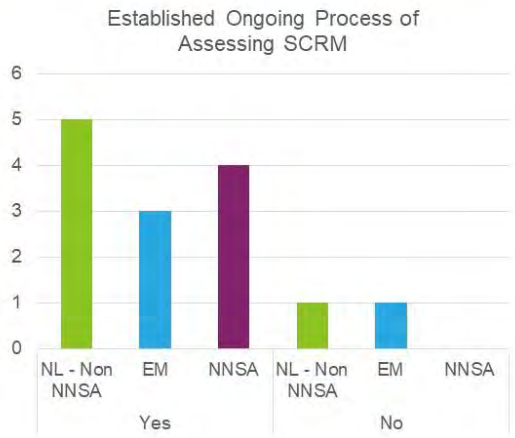
2) What level of organizational leadership has been briefed and is aware of SCRM?



4

IDAHO NATIONAL LABORATORY

3) Has your organization established an ongoing process of assessing supply chain risk?

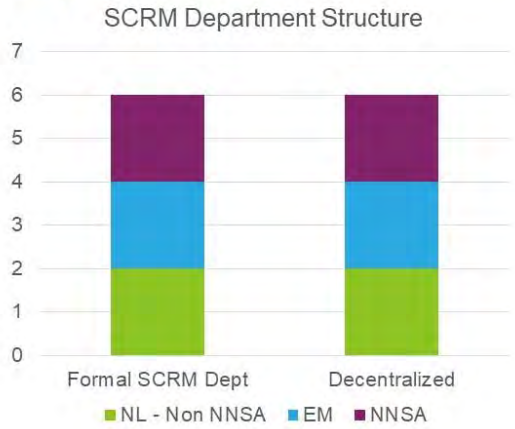


- Detail regarding process
  - Collaborating with Exiger
  - Using DNBi
  - Looking for Standardization, Centralization
  - Processes are evolving
  - Pre/Post Award Audits
  - Tracking through program reliability process

5

IDAHO NATIONAL LABORATORY

4) Does your org have a formal SCRM department or does each business directorate have separate SCRM responsibilities?

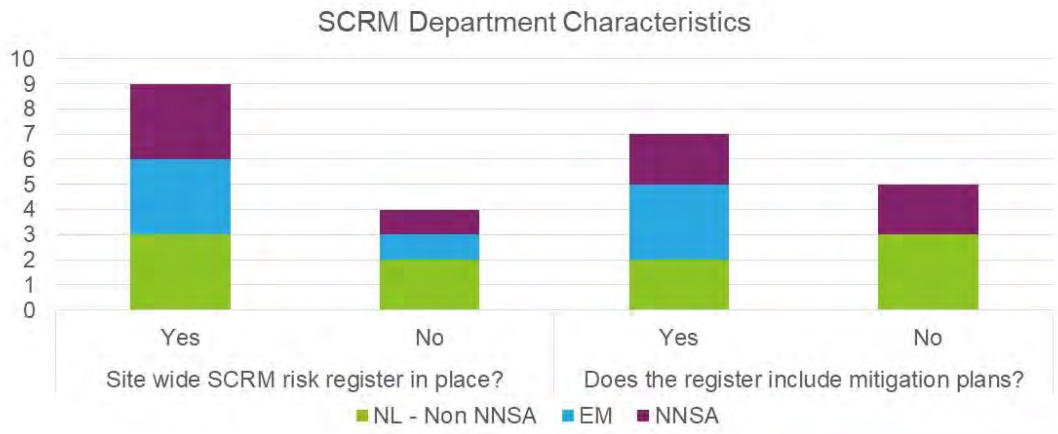


- Formal SCRM Dept
  - Managed in SCM department
  - Conducts Supplier Risk Assessments (SRAs) on mentor/protégé suppliers, strategic agreement suppliers and as directed
- Decentralized
  - Procurement, Shipping & Receiving, and Quality are all under separate directorates
  - Transparency is difficult and standards are inconsistent
  - SCRM employees double as contract analysts
  - Risk concerns: NEA concerns, export-controlled work, financial risk
  - Counterintelligence and Supplier Management office provide support for SRAs
  - Risks identified by technical managers and/or subject matter experts
  - Monthly risk meetings

6

IDAHO NATIONAL LABORATORY

4.a.b) SCRM Department Characteristics



7

IDAHO NATIONAL LABORATORY

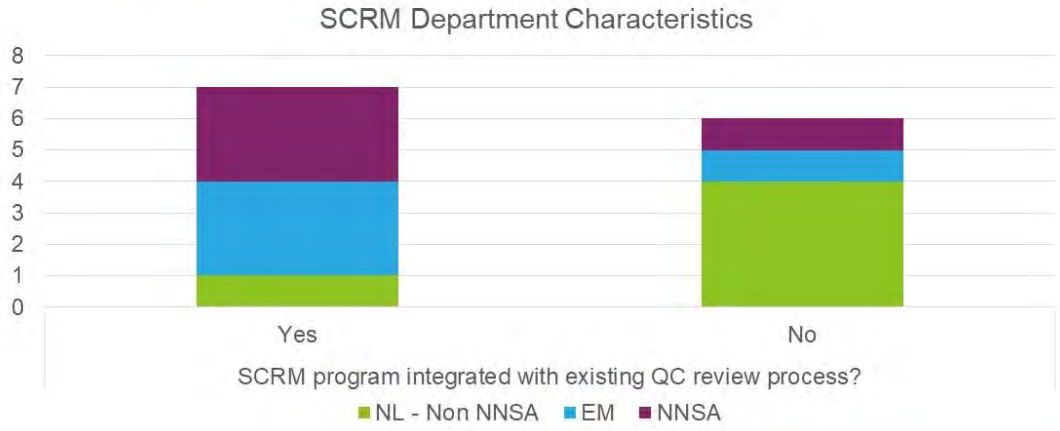
4.c) How do you prioritize risk in the supply chain?

- Followed a High, Moderate, or Low categorization based on likelihood of occurrence, consequence, and mitigation strategies
- No formal decision tree yet but is in development
- Evaluated based on mission critical areas
- Risk evaluated in two categories using a tradeoff matrix: Likelihood and Consequence
- Examples
  - **Single Source** procurements are categorized as *moderate*
  - Substantive vender engagements are classified as *risky*
  - Low level logistical vendor engagements are *not risky*
  - No-Go: debarment, inadequate Dun & Bradstreet Scores, Restricted Party Screening findings
- All types of risk are housed and maintained by Sitewide Risk Register.
  - Supplier risks and mitigation plans are included in register

8

IDAHO NATIONAL LABORATORY

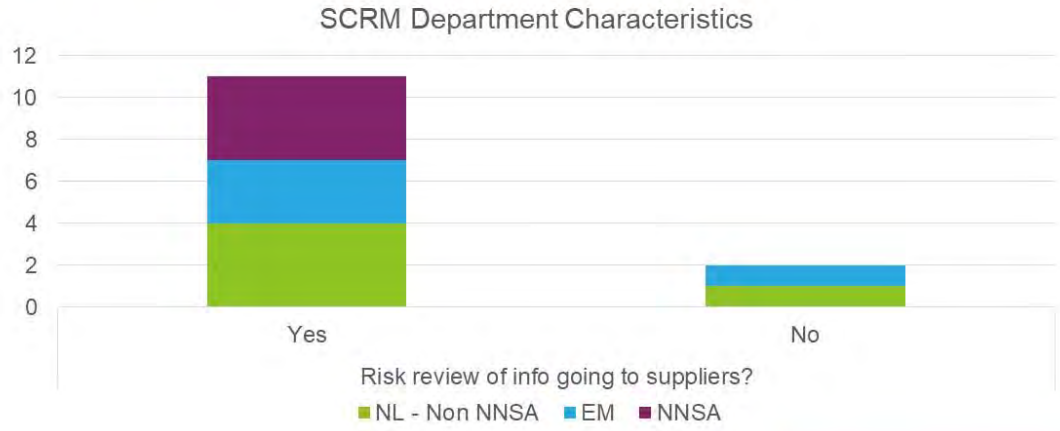
4.d) Is your program integrated with existing quality control processes?



4.d) Detail - SCRM Integration with QC Review Process?

- Yes (7 responded yes)
  - Supplier performance reports are used by SCRM in the bid process to determine necessary surveillance oversight for current/future procurements
  - Embedded in inspection programs
  - Supplier Risk Assessments performed on quality Level 1-2 suppliers
  - Qualified suppler list ensures adequate supplier base
- No (6 responded no)
  - Strong working relationship exists with Quality department to help manage performance
  - QA program is well established but plans are underway to integrate QA with SCRM

4.e) Do you perform a risk review of documents/info going to suppliers prior to sending out?



11

IDAHO NATIONAL LABORATORY

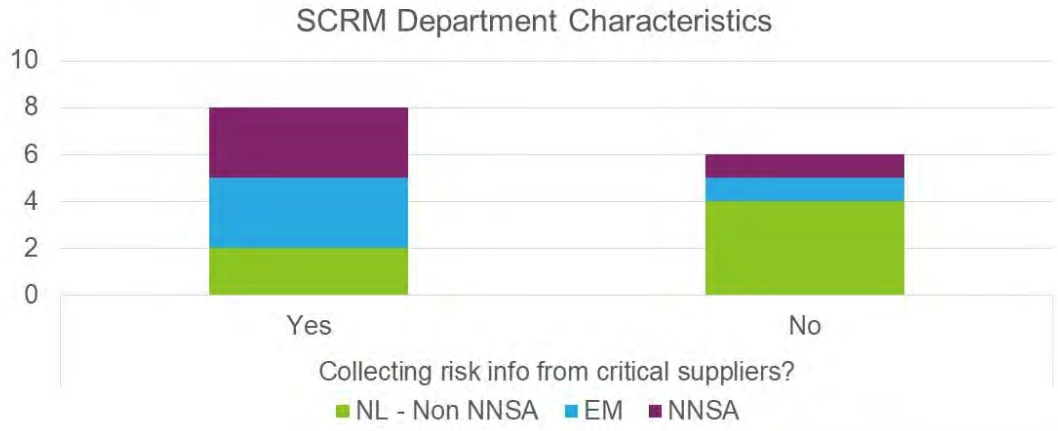
4.f) Controls implemented to prevent gratuitous info from being sent to suppliers.

- Internal Reviews
  - Semi- Annual and Annual audits
  - Compliance reviews
- Procurement Specialist and Technical Rep. Training
- Procurement reviews Statement of Work and entire requisition package to prevent sending unwanted info
- Export control department review
- Information Management Department is increasingly involved
- Disciplined document review process
- Documents reviewed by programmatic and supply chain management personnel
- Peer reviews

12

IDAHO NATIONAL LABORATORY

5) Are you periodically collecting risk information from your critical suppliers?



13

IDAHO NATIONAL LABORATORY

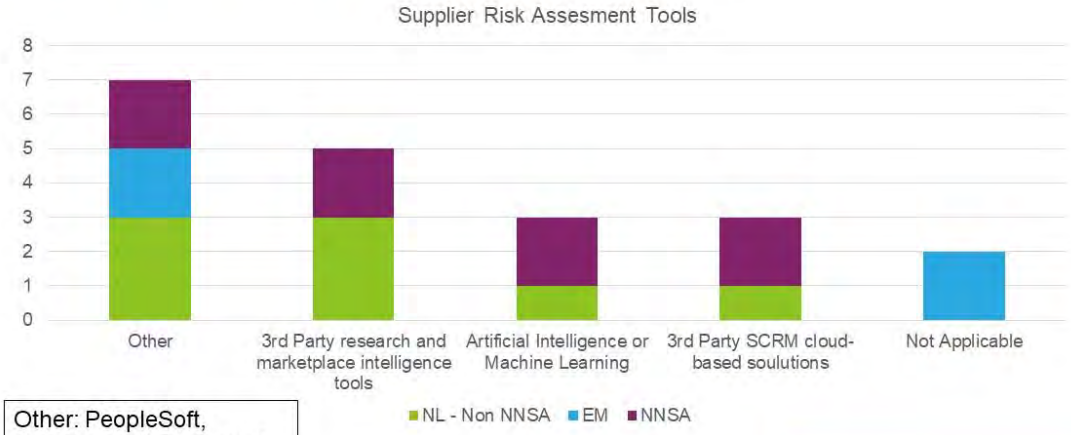
5) Detail - Actions Taken After Collecting Risk Info From Suppliers

- Run financial sanction process once a week
- Auto inactivation after 18-months of inactivity
- **Implement Request for Supplier Corrective Action process or Supplier Corrective Action Report**
- Interim and ongoing audits
- Removal from bidders' or 'do not solicit' list
- Suppliers placed on hold to require additional review prior to procurement
- Supplier Risk Assessments have expiration dates
- Follow Termination Articles in terms and conditions

14

IDAHO NATIONAL LABORATORY

6) What types of tools does your organization use to evaluate suppliers to assess risk?



Other: PeopleSoft, SAM.gov, D&B, **Internal contract reviews**

15

IDAHO NATIONAL LABORATORY

6.a) What challenges has your site faced in implementing commercially available SCRM tools?

- Exiger is not FedRamp compliant
- **FedRamp certification**
- Funding
  - Unwillingness to invest in future outcomes. Not a priority
  - For small organizations cost/benefit has not been considered or evaluated as potentially beneficial
  - Deciding when and how to resource the use of AI to support human analysts is an important decision.
- Cross functional acceptance or visibility and defining who critical suppliers are
- **Vetting and obtaining approval through IT and information security concerns**

16

IDAHO NATIONAL LABORATORY

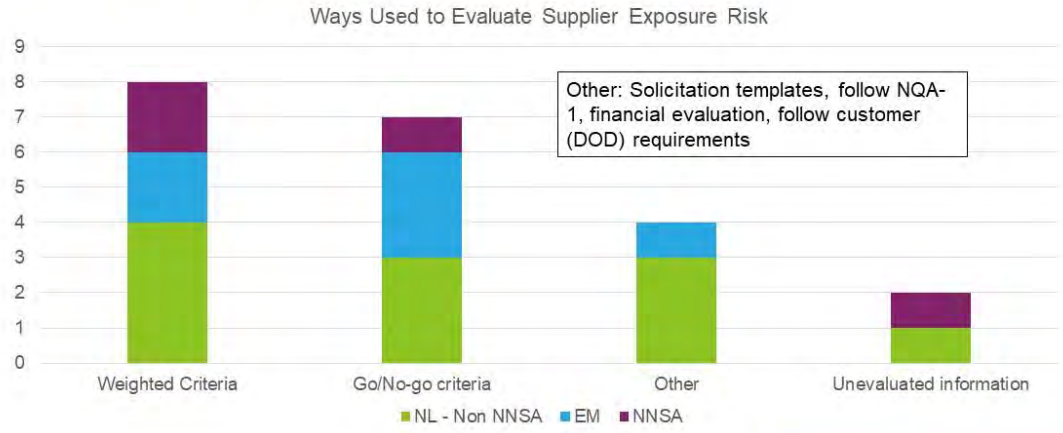
7) What corrective action techniques does your organization use for suppliers if adverse SCRM information is developed during execution?

- Corrective Action Plans
  - Plans need to outline necessary steps required for resolution along with the documentation requirements.
  - Plans are discussed with the supplier, approved, and monitored.
  - Currently corrective action plans are issued for supplier performance evaluations below 70, or for quality or safety related deficiencies. SCRM mitigation plans are envisioned for our future in which each stakeholder participates.
  - A plan for corrective action notification to suppliers communicating certain risk events related to SCRM information will need to be developed with guidance from our legal department
- For issues concerning contractual requirements,
  - issues are evaluated by the Buyer and General Counsel.
  - Follow termination articles in general provisions and terms and conditions.
  - Cure and Show Cause letters
- A scorecard system that can be shared with the supplier and internally.
- Stop-work orders
- Non-conformance reports

17

IDAHO NATIONAL LABORATORY

8) Do you analyze supplier exposure to risk in the evaluation process and how it is utilized?



18

IDAHO NATIONAL LABORATORY

9) What type of training related to SCRM does your organization provide?

10) What types of training would you find useful that could service multiple sites?

- Awareness training and clear definition of SCRM and all that applies
- General Buyer Training on QA Risk Management Process and Business Risk Management Training
- Case Studies and real-life lessons learned
- DOE sponsored SCRM software to be used across the complex
- **SCRM decision tree**
  - Stakeholder responsibility for identifying level of risk
    - Environmental, safety, export control info, PII, etc.
- Tools for SCRM analysis, proper techniques, potential threats, legal and regulatory statues.
- Do it through On-the-job training

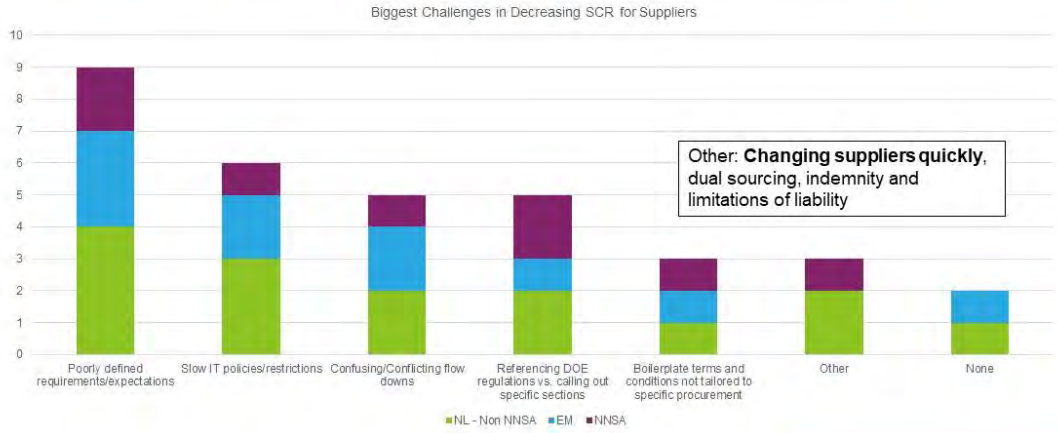
10) Training Suggestions Cont…

- Counterfeit and Cyber training
- Gray market resellers and how to authenticate
- General SCRM, NEA and S/CI training
- SCRM processes to identify, assess, prioritize, and mitigate supply chain risks
- Supplier relationship management in M&O environment
- CSR and compliance, subcontractor supply chain visibility
- Implement training on an Overall Supplier Health Score as conducted by one NNSA site

21

IDAHO NATIONAL LABORATORY

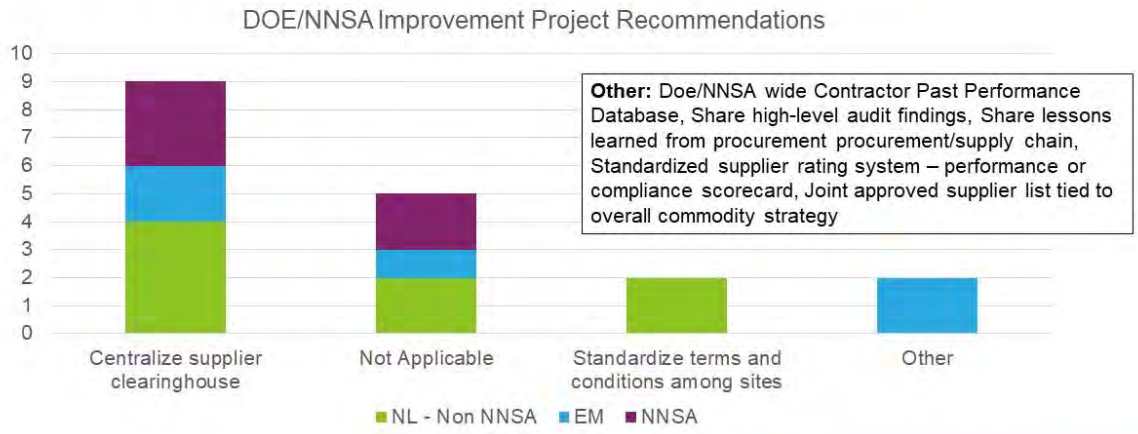
11) What do you consider your biggest challenge in decreasing Supply Chain Risk for our suppliers?



22

IDAHO NATIONAL LABORATORY

12) Which DOE/NNSA improvement project would benefit your organization/supply chain the most?



13) What is your organization's biggest need in relation to starting/improving your SCRM efforts?

- Training SCRM personnel at all levels on risk management programs
- **Available resources and funding**
- Centralized and unified SCRM flow down requirement
- **Regulatory clarity, centralization, and standardization**
- Realization that vendors don't need us as much as we need them
- Focusing on key risk elements
- Having someone to do the work
- Use of cloud-based bid data analysis tools without delay associated with FedRAMP requirement – implement solutions faster