# Nuclear Regulatory Commission
# Office of the Chief Information Officer
# Computer Security Template

| | |
|---|---|
| Office Instruction: | **CSO-TEMP-0016** |
| Office Instruction Title: | **NRC Licensee Related Supply Chain Risk Assessment Template** |
| Revision Number: | **1.0** |
| Effective Date: | **November 7, 2023** |
| Primary Contacts: | **Kathy Lyons-Burke**<br>**Senior Level Advisor for Information Security** |
| Responsible Organization: | **OCIO/CSO** |
| Summary of Changes: | CSO-TEMP-0016, "NRC Licensee Related Supply Chain Risk Assessment Template," defines the template that must be used to record the supply chain risk assessment of an NRC licensee related company. |
| ADAMS Accession No.: | ML23306A216 |

| Agency Official | Approval Signature and Date |
|---|---|
| Jon Feibus<br>Chief Information Security Officer (CISO)<br>Office of the Chief Information Officer (OCIO) | Jonathan R. Feibus<br>Digitally signed by Jonathan R. Feibus<br>Date: 2023.11.02 16:24:37 -04'00' |

# TABLE OF CONTENTS

# Computer Security Template
# CSO-TEMP-0016
NRC Licensee Related Supply Chain Risk Assessment Template

---

## 1 PURPOSE

CSO-TEMP-0016 defines the template that must be used to record the supply chain risk assessment for an NRC licensee related company. CSO-PROS-0016, "NRC Licensee Related Supply Chain Risk Assessment Process" is used to perform the assessment and the results are recorded within this template.

## 2 TEMPLATE INSTRUCTIONS

The template sections are completed by the supply chain risk management working group chair.

Placeholders in <blue> in the template should be replaced with the required information and the font color returned to black before submitting the assessment.

In some cases, the boilerplate has multiple text options. These options are provided in {green} and separated by ";". After the appropriate text is chosen, the assessor must change the font color to black and remove the brackets.

### 2.1 Template-Wide Instructions

REMOVE document instructions before filling out the template.

General placeholders are provided throughout the Supply Chain Risk Assessment (SCRA) template and should be replaced with the required information for all occurrences. A spreadsheet that contains all of the high-risk findings must be part of the ADAMS SCRA package with the documented risk assessment.

For each section in the SCRA template, replace each general placeholder with the following information:

- <ADAMS asscession #> − Provide the Agencywide Documents Access and Management System (ADAMS) accession number of the relevant document.
- <Brief description of rationale for overall risk level determination> − Provide the rationale for the assessor determined level of supply chain risk for the company.
- <Brief description of why> − Provide the rationale for the assessor determined level of supply chain risk.
- <Company Name> − Provide the exact name of the licensee related company.
- <DD Risk> – Select Low, Moderate, High, or Very High as the level of determined risk based upon the definitions identified above as the Level of Supply Chain Risk.
- <level> – replace with the Exiger risk level associated with the risk severity (e. g. LOW, MEDIUM-HIGH)

- <Key finding 1> – Identify each key finding from the study.
- <Month, Year> – Provide the full month name where “Month” appears, and the full year where “Year” appears (i.e., January, 2023).
- <n> – Replace “n” with the number that corresponds with the column header.
- <n.nn> – Replace “n.nn” with the risk severity that corresponds with the row header. 2 decimal points should be used for these values.
- <Risk Date> – Provide the date of the risk text.
- <risk level> – Provide the assessor determined level of risk for the item. The valid risk levels are: low, low-moderate, moderate, moderate-high, high.
- <Risk Title> – Provide the title identified for the risk if the risk was identified in the Summary of High Scoring Unstructured Risk Events table and with the value in the Events column if the risk was identified in the Summary of High Scoring Structured Risk Events table.
- <Brief Risk Description and Assessor Interpretation of Risk> – Provide a brief high-level summary of the full risk if the risk was identified in the Summary of High Scoring Unstructured Risk Events table and with the value in the Remarks column if the risk was identified in the Summary of High Scoring Structured Risk Events table. Then add the assessor’s interpretation of the risk.
- <SCRA Risk> – Select Low, Moderate, High, or Very High as the level of determined risk based upon the definitions identified above as the Level of Supply Chain Risk.

Make the appropriate choice as indicated below:

- {are | is}
  - Provide the correct verb that corresponds with the number.
- {No Deep Dive was performed. | Deep Dive Identified Risk: NRC tasked Exiger Government Solutions (EGS) with performing a deep dive on <Company Name>. The deep dive surfaced the following key findings:
  - Choose No Deep Dive was performed if no deep dive analyses performed are relevant to the company.
  - Choose Deep Dive Identified Risk: NRC tasked Exiger Government Solutions (EGS) with performing a deep dive on <Company Name>. The deep dive surfaced the following key findings: if deep dive analyses relevant to were performed since the last company SCRA was performed.
- {No illumination was performed. | Illumination Identified Risk: NRC tasked Exiger Government Solutions (EGS) with illuminating <Brief description of requested illumination>. The illumination surfaced the following key findings:
  - Choose No illumination was performed if no illuminations that are relevant to the company have been performed since the last company SCRA was performed.
  - Choose The illumination identified risk associated with <Company Name> includes <summary of relevant illumination findings>. The <Company Name> illumination risk is **<Illumination Risk>** if illuminations relevant to the company have been performed since the last company SCRA.

## 2.2 Headers and Footers

After replacing the placeholders in the headers and footers, check each header and footer throughout the SCRA to ensure that the placeholders were populated accurately.

## 2.3 Title Page

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

- <adj-level> – Provide the adjusted risk level as determined from the additional analysis performed as indicated in the column header.
- <Assessor Name> – Provide the full name of the individual that performed the supply chain risk assessment.
- <Assessor Org> – Provide the NRC organization for which the assessor works. If the assessor is a contractor, provide the name of the company in which the contractor is employed.
- <CISO Name> – Provide the full name of the NRC CISO.
- <NRC CISO Org> – Provide the NRC organization for which the CISO works.
- <SCRA Version Number> – Provide the latest version number of the SCRA. Use the format "N.N." Additional instructions for version numbering are provided below in Section 2.4, Document Revision History Page, of these instructions.

  **Examples:**
  Version 1.0
  Version 1.1

- <SCRA Date> – Provide the date this SCRA was completed. Use the format "Month DD, YYYY."
- The assessors must digitally sign in the space provided next to their name.

## 2.4 Executive Summary

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder in Table ES-1 with the following information:

| | |
|---|---|
| Risks Identified <n> | Provide the total number of risks identified in the DDIQ dashboard for the vendor risk area |
| Risks of Concern <n> | Provide the number of DDIQ dashboard identified risks for the vendor risk area that the assessor determined were of concern |
| Risk Severity <n.nn> | Provide the risk severity identified in the DDIQ dashboard for the vendor risk area |
| Risk Level <level> | Identify the Exiger risk level associated with the risk severity (e. g. LOW, MEDIUM-HIGH) |

| | |
|---|---|
| **[Deep Dive Adjusted Risk Levels]** <adj-level> | If one or more deep dives was conducted for this company, provide the risk level as adjusted by the contents of the deep dive(s). |

Replace each remaining placeholder with the following information:

- <Brief description of why> − Provide a brief summary of the assessor’s rationale for the identified risk level.
- <Key finding 1> − Provide a bullet for each key finding identified in the source document.

## 2.5 Table of Contents, Figures, and Tables Pages

Do not modify any of the tables directly. Update the tables when the document is completed:

- Press CTRL+A to select all text in the document.
- Press the F9 key.
- In the Update Table dialog box, click the Update Entire Table option button.

## 2.6 Company Description

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

- <assessment of company headquarters locations> – Provide the locations of the company headquarters locations fully qualified with the country the headquarters are located in.
- <Licensee Related Function/Purpose> – Provide a brief description of the licensee related company function, including when licensed by the NRC and docket number and license number, if applicable.
- <Licensee Relationship to NRC> – Provide the full relationship of the company to the NRC.

## 2.7 Risk Assessment Information Sources

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

- <CAGE> − Provide the company’s CAGE Code that was assigned by the Department of Defense's Defense Logistics Agency (DLA).
- <DUNS> − Provide the Dun & Bradstreet (D&B) DUNS unique nine-digit identifier for businesses.
- <UEI> − Provide the Unique Entity ID (UEI) is a unique identifier assigned to every company with which the Federal government does business.

## 2.8 SCRA Information Sources

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

- <Document Title> − Provide the title of the document that was used as an information source for this SCRA.
- <Unique Identifier> − Provide the unique identifier associated with the document (e.g., ADAMS accession number).
- <Document Date> − Provide the date of the document in the format: DD-Mmm-YY.
- <(URL Access Link) > − Provide the URL as a link to access the document.

## 2.9 Risks Identified

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Select the risk information that is included in the SCRA.

### 2.9.1 Overall Risk

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

-  − Replace the image with the Overall Risk dial image from the dashboard representation of the DDIQ report.
-  − Replace the image with the summary of unstructured risk events pie image from the dashboard representation of the DDIQ report.

### 2.9.2 Financial Risk

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. For the table, keep rows where high risks were identified for the risk area. Replace each remaining placeholder with the following information:

-  − Replace the image with the Average Financial Risk dial image from the dashboard representation of the DDIQ report.
- <DnB level> − Provide the word interpretation of the level associated with the identified DnB value (e.g., low).
- <Number of financial risks> − Provide the total number of financial high risks identified.
- <Number of unique financial risks of concern> − Provide the number of identitied financial high risks that were determined to be unique risks of concern.

### 2.9.3 FOCI Risk

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. For the table, keep rows where high risks were identified for the risk area. Replace each remaining placeholder with the following information:

-  − Replace the image with the Average FOCI Risk dial image from the dashboard representation of the DDIQ report.
- <Number of FOCI risks> − Provide the total number of FOCI high risks identified.
- <Number of unique FOCI risks of concern> − Provide the number of identitied FOCI high risks that were determined to be unique risks of concern.

### 2.9.4 Operational Risk

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. For the table, keep rows where high risks were identified for the risk area. Replace each remaining placeholder with the following information:

-  − Replace the image with the Average Operational Risk dial image from the dashboard representation of the DDIQ report.
- <Number of operational risks> − Provide the total number of operational high risks identified.
- <Number of unique operational risks of concern> − Provide the number of identitied operational high risks that were determined to be unique risks of concern.

### 2.9.5 Reputational, Criminal, and Regulatory Risk

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. For the table, keep rows where high risks were identified for the risk area. Replace each remaining placeholder with the following information:

-  − Replace the image with the Average RCR Risk dial image from the dashboard representation of the DDIQ report.
- <Number of RCR risks> − Provide the total number of RCR high risks identified.
- <Number of unique RCR risks of concern> − Provide the number of identitied RCR high risks that were determined to be unique risks of concern.

Deep Dive Information

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Repeat the sections for each Exiger Deep Dive that applies to the that was performed since the last system SCRA was performed. Replace each remaining placeholder with the following information:

- <Deep Dive Key Finding> – Provide each of the key findings from the company Deep Dive analysis.

- <Deep Dive ML#> – Provide the ADAMS accession number for the Deep Dive analysis.
- <Deep Dive Title> – Provide the title of the Deep Dive analysis.
- <description of purpose of the Deep Dive> – Provide the purpose of the deep dive analysis.
- <Discussion of overall Deep Dive risk> – Provide a succinct discussion of the risk across all of the Deep Dive analyses.
- <Discussion of resulting DD risk> – Provide the basis for the resulting Deep Dive risk level.
- <summary of relevant Deep Dive findings> – Provide a summary of all of the relevant deep dive findings.

Make the appropriate choice as indicated below:

- {No Deep Dive was performed for <Company Name>. | The Deep Dive identified risk associated with <Company Name> includes <summary of relevant Deep Dive findings>.
  - Choose No Deep Dive was performed for <Company Name> if no deep dive analyses performed are relevant to the company.
  - Choose The Deep Dive identified risk associated with <Company Name> includes <summary of relevant Deep Dive findings>. if deep dive analyses relevant to were performed since the last company SCRA was performed.

## 2.10 Illumination Information

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Repeat the sections for each Exiger illumination that applies to the system that was performed since the last system SCRA was performed. Replace each remaining placeholder with the following information:

- <description of purpose of the illumination> – Provide the reason why the illumination was produced.
- <Discussion of illumination resulting risk> – Provide a description of the overall risk identified in the illumination and the risk relationship to NRC.
- <Discussion of overall Illumination risk> – Provide a succinct discussion of the risk across all of the illuminations.
- <Illumination Key Findings> – Provide the key findings from the illumination.
- <Illumination ML#> – Provide the ADAMS accession number of the illumination.
- <Illumination Title> – Provide the exact title of the illumination that was performed.
- <summary of relevant Illumination findings> – Provide a summary of all of the relevant findings from the illuminations performed.

Make the appropriate choice as indicated below:

- {There are no applicable Illuminations related to <Company Name>. | The illumination identified risk associated with <Company Name> includes <summary of relevant illumination findings>.}
  - Choose There are no applicable Illuminations related to <Company Name> if no illuminations that are relevant to the company have been performed since the last company SCRA was performed.
  - Choose The illumination identified risk associated with <Company Name> includes <summary of relevant illumination findings> if illuminations relevant to the company have been performed since the last company SCRA.

## 2.11 Risk Determination

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

- <summary of relevant Deep Dive findings> – Provide a succinct summary of the risk findings across all of the Deep Dive analyses relevant to <System Acronym>.
- <summary of relevant illumination findings> – Provide a succinct summary of the risk findings across all of the Illuminations relevant to <System Acronym>.

Make the appropriate choice as indicated below:

- {There are no unique risks identified for <Company Name> | There were <n> unique risks identified for <Company Name>:
  - Choose There are no unique risks identified for <Company Name> if none of the information sources revealed any unique risks for the company.
  - Choose There were <n> unique risks identified for <Company Name> if there were unique risks identified for the company.

The overall <Company Name> level of supply chain risk is determined to be **<SCRA Risk>**.

## 2.12 Appendix A Acronyms

Update the table with any additional acronyms that are in the document.

## 2.13 Appendix B References

Update the references appendix to include any sources used in performing the SCRA.

## 2.14 Document Revision History Page

Revisions must be in chronological order starting with the newest revision as the first row of the table. The initial release of the SCRA should begin with “Version 1.0.” Minor changes should increase the version number by 0.1. Major changes should increase the version number to the next applicable whole number. Only released versioning should be used. For example, if

modifications to the document are made by writers/reviewers before release, they would not be separate versions.

**Examples:**

| | |
|---|---|
| Major Update | Version 2.0 |
| Minor Update #2 | Version 1.2 |
| Minor Update #1 | Version 1.1 |
| Initial Release | Version 1.0 |

Leave the standard boilerplate text. Supply the specified text for each general placeholder as indicated in the template-wide instructions. Replace each remaining placeholder with the following information:

- <Description> - Provide a brief description of the revisions that were made to the SCRA.
- <Method> - Provide the method being used to notify stakeholders about the revision.

  **Examples:**

  Use the phrase “Initial Release” if this is the first version of the SCRA.

  Revised SCRA to reflect changes to the identified risk.

- Replace <Name/Org> with the name(s) of the individual responsible for the document revision and the organization for which they work (e.g., NRC office, region, or contractor company). In the case of the Office of the Chief Information Officer, provide the division and branch name.
- <nn-Ddd-yy> - Replace nn with the double digit day (e.g., 01, 21). Replace Ddd with the 3-letter representation of the month (e.g., Jan, Fed). Replace yy with the last 2 digits of the year (e.g., 21, 22).
- <Ver> - Replace Ver with the correct document version.

# APPENDIX A ACRONYMS

| | |
|---|---|
| ADAMS | Agencywide Documents Access and Management System |
| ASCA | Authorization System Cybersecurity Assessment |
| BIA | Business Impact Analysis |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| COOP | Continuity of Operations Plan |
| CSIRT | Computer Security Incident Response Team |
| D&B | Dun & Bradstreet |
| DCISO | Deputy Chief Information Security Officer |
| DHS | Department of Homeland Security |
| DLA | Department of Defense's Defense Logistics Agency |
| FHE | Federal HVA Enterprise |
| FIPS | Federal Information Processing Standard |
| FITARA | Federal Information Technology Acquisition Reform Act |
| FOCI | Foreign Ownership, Control, and Influence |
| HVA | High Value Asset |
| ICT | Information and Communications Technology |
| ISA | Information Security Architecture |
| ISP | Internet Service Provider |
| ISSM | Information System Security Manager |
| MEF | Mission Essential Function |
| NDAA | National Defense Authorization Act |
| NEF | National Essential Functions |
| NIST | National Institute of Standards and Technology |

| | |
|---|---|
| OCIO | Office of the Chief Information Officer |
| OMB | Office of Management and Budget |
| OUO | Official Use Only |
| PMEF | Primary Mission Essential Functions |
| PMO | Program Management Office |
| POA&M | Plan of Action and Milestones |
| PSCA | Periodic System Cybersecurity Assessment |
| SAM | System for Award Management |
| SCA | System Cybersecurity Assessment |
| SCRA | Supply Chain Risk Assessment |
| SCRM | Supply Chain Risk Management |
| SDLC | System Development Lifecycle |
| SP | NIST Special Publication |
| SR | NIST SP 800-53r5 Supply Chain Risk Management Controls |
| SRI | Nuclear Security Related Information |
| UEI | Unique Entity ID |

## CSO-TEMP-0016 Change History

| Date | Version | Description of Changes | Method Used to Announce & Distribute | Training |
|---|---|---|---|---|
| 30-Oct-23 | 1.0 | Initial release | Monthly Office Meetings. | None needed. |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

U.S. Nuclear Regulatory Commission

# <Company Name>

# NRC Licensee Related Supply Chain Risk Assessment

# Version <SCRA Version Number>

# <SCRA Date>

**Accession Number:** <ADAMS asscession #>

| Assessors | Signature and Date |
|---|---|
| **Risk Assessor:**<br><Assessor Name><br><Assessor Org> | |
| **CISO:**<br><CISO Name><br><NRC CISO Org> | |

# EXECUTIVE SUMMARY

This Supply Chain Risk Assessment (SCRA) was performed to identify supply chain risks associated with an NRC licensee. SCRAs are conducted by a supply chain risk assessor utilizing a data analytics solution to assess possible supply chain risks.

This report outlines the risks associated with <Company Name>, and Table ES-1 provides the impact level summary.

Table ES-1: <Company Name> SCRA Summary

| Risk Area | Risks Identified | Risks of Concern | Risk Severity | Risk Level | [Deep Dive Adjusted Risk Levels] |
|---|---|---|---|---|---|
| Financial Risk | <n> | <n> | <n.nn> | <level> | <adj-level> |
| Foreign Ownership, Control, and Influence (FOCI) Risk | <n> | <n> | <n.nn> | <level> | <adj-level> |
| Operational Risk | <n> | <n> | <n.nn> | <level> | <adj-level> |
| Reputational, Criminal, and Regulatory (RCR) Risk | <n> | <n> | <n.nn> | <level> | <adj-level> |
| **Overall Risk** | **<n>** | **<n>** | **<n.nn>** | **<level>** | **<adj-level>** |

Financial Risk: The overall risk of the identified financial risks of concern is <risk level>. <Brief description of why>.

FOCI Risk: The overall risk of the identified FOCI risks of concern is <risk level>. <Brief description of why>.

Operational Risk: The overall risk of the identified operational risks of concern is <risk level>. <Brief description of why>.

Reputational, Criminal, and Regulatory Risk: The overall risk of the identified reputational, criminal, and regulatory risks of concern is <risk level>. <Brief description of why>.

{No Deep Dive was performed. | Deep Dive Identified Risk:

NRC tasked Exiger Government Solutions (EGS) with performing a deep dive on <Company Name>.

The deep dive surfaced the following key findings:

- <Key finding 1>
- <Key finding 2>
- <Key finding 3>}

{No illumination was performed. | Illumination Identified Risk:

NRC tasked Exiger Government Solutions (EGS) with illuminating <Brief description of requested illumination>.

The illumination surfaced the following key findings:

- <Key finding 1>
- <Key finding 2>
- <Key finding 3>}

**Overall Risk:** The overall risk of the identified risks of concern is **<SCRA Risk>**. <Brief description of rationale for overall risk level determination>.

# Table of Contents

# Table of Tables



# Table of Figures

# 1 INTRODUCTION

The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018) requires all agencies to assess, avoid, mitigate, accept, or transfer supply chain risks; and Executive Order 14028 requires Federal agencies to enhance software supply chain security.

Supply chain risk profiles must be continually assessed for evolving threats, and prioritization of resources should flow to those areas where the impact would be unacceptably great.

While the risk of compromise is inherent in any technology that collects sensitive data or otherwise has access to critical systems, the risk increases considerably when the technology is produced or supplied by a company that could be persuaded or readily coerced to access that data or abuse that access on behalf of a foreign adversary.

## 1.1 Purpose

This Supply Chain Risk Assessment (SCRA) was performed to identify supply chain risks associated with an NRC licensee related company. SCRAs are conducted by a supply chain risk assessor utilizing a data analytics solution to assess possible supply chain risks.

## 1.2 <Company Name> Description

<Company Name> <Licensee Related Function/Purpose>

<Licensee Relationship to NRC>

<Company Name> headquarters {are | is} located in <assessment of company headquarters locations>.

## 1.3 Risk Assessment Information Sources

The Dun & Bradstreet (D&B) DUNS Number is a unique nine-digit identifier for businesses. This number is assigned once D&B identifies a company as being unique from any other in the D&B Data Cloud. The DUNS Number is used as the starting point for any company's Live Business Identity; the most comprehensive and continually updated view of any company in the Data Cloud.

The <Company Name> DUNS Number is: <DUNS #>.

A CAGE Code is assigned by the Department of Defense (DOD) Defense Logistics Agency (DLA) and represents a company's physical address for GSA mailings, payments, and administrative records. Government agencies may also use CAGE Codes to verify a security clearance or for a pre-award survey. A company needs a CAGE Code to sell to the government.

The <Company Name> CAGE Code is: <CAGE Code>.

A Unique Entity Identifier (UEI) is a number issued by the System for Award Management (SAM) to identify businesses and other entities that do business with the federal government.

The <Company Name> UEI number is: <UEI #>

## 1.4 SCRA Information Sources

Following are the information sources used to develop this SCRA for <Company Name>:

- <Document Title>, <Unique Identifier>, <Document Date>, <(URL Access Link)>
- <Document Title>, <Unique Identifier>, <Document Date>, <(URL Access Link)>

# 2 RISKS IDENTIFIED

A risk analysis has been developed for the <Company Name> supply chain risk assessment and is attached to this report. The following items, available in the DDIQ dashboard, were included in the risk analysis:

- [Unstructured Risk Events]
- [Structured Risk Events]
- [Watchlist Detail Structure]
- [Foreign Risk Breakdown]
- [Ownership Target Values]
- [Section 889 Mentions]
- [Industry Breakdown]
- [Federal Government Notices]

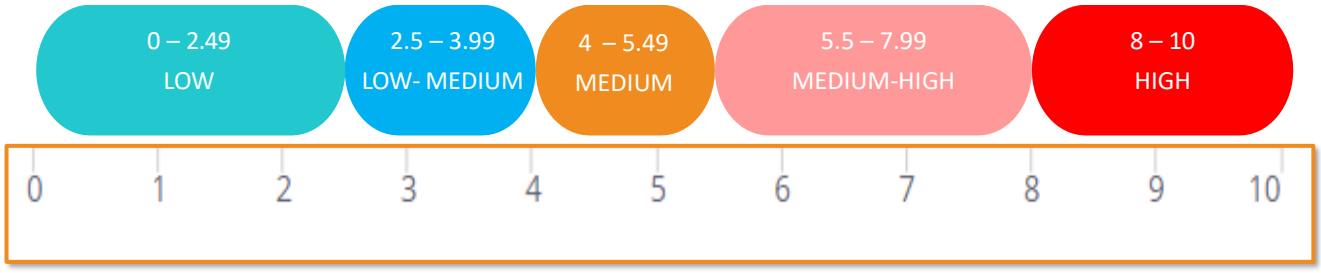
The Exiger risk scoring is performed in accordance with Figure 1: Exiger Risk Scoring Values.

## 2.1 Overall Risk

The overall risk associated with <Company Name> is <risk level>.

Figure 2 represents the overall risk associated with <Company Name>, and Figure 3 provides a pie chart breakout of the unstructured risk events. The overall risk is determined using the weighted values of the FOCI (40%), the average financial risk (10%), the average operational

Figure 1: Exiger Risk Scoring Values




risk (25%), and the average reputational risk (25%).

Figure 2: <Company Name> Overall Risk

The Overall Risk associated with <Company Name> is <risk level>.

Figure 3: <Company Name> Summary of Unstructured Risk Events

## 2.2 Financial Risk

Financial management can either build or erode an organization's ability to deliver as a service provider. Figure 4 shows the average financial risk for <Company Name>.

Figure 4: <Company Name> Average Financial Risk

The average <Company Name> financial risk level is <risk level>.

D&B evaluates the sustainability and payment behavior of a company by assessing the risk of failure and the risk of slow-to-severely-delinquent payments through scores, ratings, and indices.

Viability rankings range from 1-9, where 9 represents the highest risk of going out of business or becoming inactive and 1 represents the lowest risk. For the purposes of this report, green is considered to be low (1-4), light orange is considered to be medium (5-6), dark orange is considered to be high (7), and red is considered to be very high (8-9).


Figure 5: Credit Risk Scale

The <Company Name> Corporate D&B Credit Risk is <n>, which is a <DnB level> level.

Table 1 summarizes the Financial risks identified for <Company Name>.

Table 1: Financial Identified High Risks

| Risk Area | Risks Identified | Risks of Concern |
|---|---|---|
| [Asset Freeze] | <n> | <n> |
| [Bankruptcy Related] | <n> | <n> |
| [Central Bank Reprimands] | <n> | <n> |
| [Counterfeit] | <n> | <n> |
| [Credit Downgrade] | <n> | <n> |
| [Divestment] | <n> | <n> |
| [Financial Crime] | <n> | <n> |
| [Financial Issue] | <n> | <n> |
| [Financial Regulator] | <n> | <n> |
| [Fine or Penalty Imposed] | <n> | <n> |
| [Flagged Financial] | <n> | <n> |
| [Indicator of Wealth] | <n> | <n> |
| [Insolvency] | <n> | <n> |
| [Liquidation] | <n> | <n> |
| [Money Laundering] | <n> | <n> |
| [Offshore Account] | <n> | <n> |
| [Provided Funding To] | <n> | <n> |
| [Received Funding From] | <n> | <n> |
| [Relative or Associate] | <n> | <n> |
| [Sec Investment Advisor] | <n> | <n> |
| [Source of Wealth] | <n> | <n> |
| [Stock Analysis] | <n> | <n> |
| [Stock Exchange] | <n> | <n> |
| [Tax Issue] | <n> | <n> |
| **Overall Risk** | **<n>** | **<n>** |

### 2.2.1 Assessor Financial Risk Summary

The risk assessment identified <Number of financial risks> financial high risks for <Company Name>. Of these, <Number of unique financial risks of concern> were determined to be unique risks of concern. The overall risk of the identified financial risks of concern is <risk level>.

Detailed information for each identified unique risk of concern is documented below.

#### 2.2.1.1 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.2.1.2 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.2.1.3 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

## 2.3 Foreign Ownership, Control, and Influence (FOCI) Risk

FOCI risk existence and impact is often opaque or obfuscated. Influence can be exerted through partnerships, business ties, reliance, or operational dependence. Additional risk indicators lie in funding sources, manufacturing, or logistics vulnerability based on regional disasters, climate changes, geopolitical tensions, or adversarial interests. Figure 6 shows the average FOCI risk for <Company Name>.

Figure 6: <Company Name> Average FOCI Risk

The average <Company Name> FOCI risk level is <risk level>.

Table 2 summarizes the FOCI risks identified for <Company Name>.

Table 2: FOCI Identified High Risks

| Risk Area | Risks Identified | Risks of Concern |
|---|---|---|
| [Business SOE] | <n> | <n> |
| [Entity Acquired By] | <n> | <n> |
| [External Trade Regulator] | <n> | <n> |
| [Links to Risk Sensitive Jurisdiction] | <n> | <n> |
| [Links to Sanctioned Jurisdiction] | <n> | <n> |
| [Merger/Acquisition] | <n> | <n> |
| [Parent] | <n> | <n> |
| [Privatization of State Owned Company] | <n> | <n> |
| [Sanctioned Country] | <n> | <n> |
| [State Owned Company] | <n> | <n> |
| [Subsidiary] | <n> | <n> |
| [Foreign Risk Breakdown] | <n> | <n> |
| **Overall Risk** | **<n>** | **<n>** |

### 2.3.1 Assessor FOCI Risk Summary

The risk assessment identified <Number of FOCI risks> FOCI high risks for <Company Name>. Of these, <Number of unique FOCI risks of concern> were determined to be unique risks of concern. The overall risk of the identified FOCI risks of concern is <risk level>.

Detailed information for each identified risk of concern is documented below.

#### 2.3.1.1 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.3.1.2 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.3.1.3 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

## 2.4 Operational Risk

A third-party's operational weakness can impact their ability to deliver. Infrastructure resilience, cybersecurity hygiene, and management of human capital are risk indicators an organization can monitor for managing third-party risk. Figure 7 shows the average operational risk for <Company Name>.

Figure 7: <Company Name> Average Operational Risk

The average <Company Name> FOCI risk level is <risk level>.

Table 3 summarizes Operational risks identified for <Company Name>.

Table 3: Operational Identified High Risks

| Risk Area | Risks Identified | Risks of Concern |
|---|---|---|
| [Certification]. | <n> | <n> |
| [Data Breach] | <n> | <n> |
| [Decertification] | <n> | <n> |
| [Employee Retention] | <n> | <n> |
| [Government Contractor] | <n> | <n> |
| [Government Department] | <n> | <n> |
| [High Risk Industry] | <n> | <n> |
| [Industry Regulator] | <n> | <n> |
| [International Sanctions] | <n> | <n> |
| [Key Hire] | <n> | <n> |
| [Labor Issues] | <n> | <n> |
| [Layoff] | <n> | <n> |

Table 3: Operational Identified High Risks

| Risk Area | Risks Identified | Risks of Concern |
|---|---|---|
| [Management Issue] | <n> | <n> |
| [Management Reference] | <n> | <n> |
| [Moved Location] | <n> | <n> |
| [Negative Performance] | <n> | <n> |
| [Occupational Safety Issue] | <n> | <n> |
| [Risk Sensitive Industry] | <n> | <n> |
| [Risk Sensitive Jurisdiction] | <n> | <n> |
| [Safety Issue] | <n> | <n> |
| [Sanctions] | <n> | <n> |
| [Significant Mention] | <n> | <n> |
| [Sustainable Risk Industry] | <n> | <n> |
| **Overall Risk** | **<n>** | **<n>** |

### 2.4.1 Assessor Operational Risk Summary

The risk assessment identified <Number of Operational risks> Operational high risks for <Company Name>. Of these, <Number of unique Operational risks of concern> were determined to be unique risks of concern. The overall risk of the identified Operational risks of concern is <risk level>.

Detailed information for each identified risk of concern is documented below.

#### 2.4.1.1 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.4.1.2 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.4.1.3 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

## 2.5 Reputational, Criminal, and Regulatory Risk

Reputational, Criminal, and Regulatory (RCR) risk can impact an organization's ability to deliver. Monitoring adverse media, criminal records, suspensions, debarments, defective pricing, regulatory enforcements, defective pricing, regulatory enforcement actions, sanctions, and import/export violations are all effective means for managing third-party risk. Figure 8 shows the average operational risk for <Company Name>.

Figure 8: <Company Name> Average Reputational, Criminal, and Regulatory Risk

The average <Company Name> RCR risk level is <risk level>.

Table 4 summarizes RCR risks identified for <Company Name>.

Table 4: Reputational, Criminal, and Regulatory Risk Identified High Risks

| Risk Area | Risks Identified | Risks of Concern |
|---|---|---|
| [Adverse] | <n> | <n> |
| [Associated With Scandal] | <n> | <n> |
| [Award] | <n> | <n> |
| [Cannabis Business] | <n> | <n> |
| [Child Abuse] | <n> | <n> |
| [Child Sex Abuse] | <n> | <n> |
| [Client Retention] | <n> | <n> |
| [Company Overview] | <n> | <n> |
| [Consumer Complaints] | <n> | <n> |
| [Conviction] | <n> | <n> |
| [Corruption] | <n> | <n> |
| [Discrimination] | <n> | <n> |
| [Disqualification] | <n> | <n> |
| [Drug Crime] | <n> | <n> |

Table 4: Reputational, Criminal, and Regulatory Risk Identified High Risks

| Risk Area | Risks Identified | Risks of Concern |
|---|---|---|
| [Environmental Crime] | <n> | <n> |
| [Flagged Criminal] | <n> | <n> |
| [Flagged Reputational] | <n> | <n> |
| [Fraudulent Activity] | <n> | <n> |
| [Homicide] | <n> | <n> |
| [Human Rights] | <n> | <n> |
| [Human Trafficking] | <n> | <n> |
| [Investigation Related] | <n> | <n> |
| [Kidnapping] | <n> | <n> |
| [Labor Violations] | <n> | <n> |
| [Law Enforcement Action] | <n> | <n> |
| [Legal Issue] | <n> | <n> |
| [Legal Risk] | <n> | <n> |
| [Organized Crime] | <n> | <n> |
| [Political Exposure] | <n> | <n> |
| [Political Relation Company] | <n> | <n> |
| [Politically Exposed Person] | <n> | <n> |
| [Potential Political Exposure] | <n> | <n> |
| [Product Issues] | <n> | <n> |
| [Regulatory Action] | <n> | <n> |
| [Regulatory Enforcement] | <n> | <n> |
| [Regulatory Site] | <n> | <n> |
| [Reputational Issue] | <n> | <n> |
| [Sexual Assault] | <n> | <n> |
| [Terrorism] | <n> | <n> |
| [Torture] | <n> | <n> |
| [Violation Related] | <n> | <n> |
| [Wanted Person] | <n> | <n> |
| [Watch List] | <n> | <n> |
| **Overall Risk** | **<n>** | **<n>** |

### 2.5.1 Assessor Reputational, Criminal, and Regulatory Risk Summary

The risk assessment identified <Number of RCR risks> RCR high risks for <Company Name>. Of these, <Number of unique RCR risks of concern> were determined to be unique risks of concern. The overall risk of the identified RCR risks of concern is <risk level>.

Detailed information for each identified risk of concern is documented below.

#### 2.5.1.1 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.5.1.2 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

#### 2.5.1.3 <Risk Title>

**Risk Date:** <Risk Date>

<Brief Risk Description and Assessor Interpretation of Risk>

This risk presents a <risk level> risk.

# 3 <COMPANY NAME> DEEP DIVE

The Exiger Deep Dive is an Enhanced Due Diligence Report, which are reports produced by Exiger's team of analysts and subject matter experts that:

- Fully trace back and map ultimate beneficial ownership
- Incorporate DDIQ profile data and external data sources covering additional trade data, visa sponsorship information, software vendor and sales networks, cyberhygiene, and cybersecurity evaluations

{No Deep Dives was performed for <Company Name>. | The Deep Dive identified risk associated with <Company Name> includes <summary of relevant Deep Dive findings>.

## 3.1 <Deep Dive Title>

In <Month, Year>, Exiger <description of purpose of the Deep Dive> (<Deep Dive ML#>).

The Deep Dive identified the following key findings:

1. <Deep Dive Key Finding>
2. <Deep Dive Key Finding>
3. <Deep Dive Key Finding>

<Discussion of resulting DD risk>. The <Deep Dive Title> Deep Dive risk is **<DD Risk>**.

### 3.2 <Deep Dive Title>

In <Month, Year>, Exiger <description of purpose of the Deep Dive> (<Deep Dive ML#>).

The Deep Dive identified the following key findings:

1. <Deep Dive Key Finding>
2. <Deep Dive Key Finding>
3. <Deep Dive Key Finding>

<Discussion of resulting DD risk>. The <Deep Dive Title> Deep Dive risk is **<DD Risk>**.

### 3.3 <Deep Dive Title>

In <Month, Year>, Exiger <description of purpose of the Deep Dive> (<Deep Dive ML#>).

The Deep Dive identified the following key findings:

1. <Deep Dive Key Finding>
2. <Deep Dive Key Finding>
3. <Deep Dive Key Finding>

<Discussion of resulting DD risk>. The <Deep Dive Title> Deep Dive risk is **<DD Risk>**.

### 3.4 Deep Dive Summary

<Discussion of overall Deep Dive risk>. The <Company Name> Deep Dive risk is **<DD Risk>**.

## 4 ILLUMINATION INFORMATION

An Illumination is a product produced by Exiger Subject Matter Experts that provides a macro/large-scale identification, assessment, and visualization of a program, product, or sectoral supply chain.

{There are no applicable Illuminations related to <Company Name>. | The illumination identified risk associated with <Company Name> includes <summary of relevant illumination findings>.}

### 4.1 <Illumination Title>

In <Month, Year>, Exiger <description of purpose of the illumination> (<Illumination ML#>).

The illumination identified the following key findings related to products <Company Name> uses:

- <Illumination Key Finding>
- <Illumination Key Finding>
- <Illumination Key Finding>

<Discussion of illumination resulting risk> The <Illumination Title> illumination risk identified for <Company Name> is **<Illumination Risk>**.

### 4.2 <Illumination Title>

In <Month, Year>, Exiger <description of purpose of the illumination> (<Illumination ML#>).

The illumination identified the following key findings related to products <Company Name> uses:

- <Illumination Key Finding>
- <Illumination Key Finding>
- <Illumination Key Finding>

<Discussion of illumination resulting risk> The <Illumination Title> illumination risk identified for <Company Name> is **<Illumination Risk>**.

### 4.3 <Illumination Title>

In <Month, Year>, Exiger <description of purpose of the illumination> (<Illumination ML#>).

The illumination identified the following key findings related to products <Company Name> uses:

- <Illumination Key Finding>
- <Illumination Key Finding>
- <Illumination Key Finding>

<Discussion of illumination resulting risk> The <Illumination Title> illumination risk identified for <Company Name> is **<Illumination Risk>**.

### 4.4 Illumination Summary

<Discussion of overall Illumination risk>. The <Company Name> Illumination risk is **<Illumination Risk>**.

## 5 RISK DETERMINATION

{There are no unique risks identified for <Company Name> | There were <n> unique risks identified for <Company Name>:

- <Brief description of risk>
- <Brief description of risk>}

The overall <Company Name> level of supply chain risk is determined to be **<SCRA Risk>**.

# APPENDIX A ACRONYMS

| | |
|---|---|
| ADAMS | Agencywide Documents Access and Management System |
| ASCA | Authorization System Cybersecurity Assessment |
| BIA | Business Impact Analysis |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| COOP | Continuity of Operations Plan |
| CSIRT | Computer Security Incident Response Team |
| D&B | Dun & Bradstreet |
| DCISO | Deputy Chief Information Security Officer |
| DHS | Department of Homeland Security |
| DLA | Department of Defense's Defense Logistics Agency |
| FHE | Federal HVA Enterprise |
| FIPS | Federal Information Processing Standard |
| FITARA | Federal Information Technology Acquisition Reform Act |
| FOCI | Foreign Ownership, Control, and Influence |
| HVA | High Value Asset |
| ICT | Information and Communications Technology |
| ISA | Information Security Architecture |
| ISP | Internet Service Provider |
| ISSM | Information System Security Manager |
| MEF | Mission Essential Function |
| NDAA | National Defense Authorization Act |
| NEF | National Essential Functions |

| | |
|---|---|
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OMB | Office of Management and Budget |
| OUO | Official Use Only |
| PMEF | Primary Mission Essential Functions |
| PMO | Program Management Office |
| POA&M | Plan of Action and Milestones |
| PSCA | Periodic System Cybersecurity Assessment |
| SAM | System for Award Management |
| SCA | System Cybersecurity Assessment |
| SCRA | Supply Chain Risk Assessment |
| SCRM | Supply Chain Risk Management |
| SDLC | System Development Lifecycle |
| SP | NIST Special Publication |
| SR | NIST SP 800-53r5 Supply Chain Risk Management Controls |
| SRI | Nuclear Security Related Information |
| UEI | Unique Entity ID |

# APPENDIX B REFERENCES

## LAWS AND EXECUTIVE ORDERS

[CLINGER] Clinger-Cohen Act (P.L. 104-106), February 1996, https://www.govinfo.gov/app/details/PLAW-104publ106

[EO 13806] EO 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," September 2018. https://www.federalregister.gov/documents/2017/07/26/2017-15860/assessing-and-strengthening-the-manufacturing-and-defense-industrial-base-and-supply-chain

[EO 13873] EO 13873, "Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[EO 14028] EO 14028, Improving the Nation's Cybersecurity, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[FASCSA] Federal Acquisition Supply Chain Security Act of 2018 (41 U.S.C. 1322) https://www.govinfo.gov/content/pkg/PLAW-115publ390/html/PLAW-115publ390.htm

[FISMA] Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283

[FITARA] Federal Information Technology Acquisition Reform Act (P.L. 115-88), November 2017. https://www.govinfo.gov/app/details/PLAW-115publ88

[NDAA-889] FY 2019 National Defense Authorization Act Section 889, https://www.congress.gov/bill/115th-congress/house-bill/5515/text

[TAA] Trade Agreement Act (TAA) (19 U.S.C. & 2501-2581), https://uscode.house.gov/view.xhtml?path=/prelim@title19/chapter13&edition=prelim

## POLICIES, REGULATIONS, DIRECTIVES, AND INSTRUCTIONS

[OMB A-123] Office of Management and Budget Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 2016. https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[OMB A-130] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[OMB-M-17-09] M-17-09, "Management of Federal High Value Assets" https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-09.pdf

[OMB-M-19-03] M-19-03, “Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program” https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[OMB-M-21-30] M-21-30, “Protecting Critical Software Through Enhanced Security Measures” https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf

[OMB-M-22-18] M-22-18, “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices” https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[OMB-M-23-13] M-23-13, “No TikTok on Government Devices” Implementation Guidance” https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf

[OMB-M-23-16] M-23-16, “Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices” https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf

## STANDARDS, GUIDELINES, AND REPORTS

[FIPS 199] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

[SP 800-30] NIST SP 800-30, “Guide for Conducting Risk Assessments”, Revision 1, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[SP 800-37] NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, December 2019. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-53] NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP 800-161] NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2022. https://doi.org/10.6028/NIST.SP.800-161r1

## NRC DOCUMENTS

[CSO-PLAN-0100] CSO-PLAN-0100, “Enterprise Risk Management Program Plan” https://adamsxt.nrc.gov/navigator/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId={AAD5EA3D-E57E-4499-B966-5C7CB8E6831B}&ForceBrowserDownloadMgrPrompt=false

| | |
|---|---|
| [CSO-PROS-2102] | CSO-PROS-2102, "System Cybersecurity Assessment Process" https://adamsxt.nrc.gov/navigator/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId={85620A61-72BA-C6A3-85B5-7FAC97B00000}&ForceBrowserDownloadMgrPrompt=false |
| [ICT Risk Tolerance] | Information and Communications Technology Risk Tolerance, Revision 1.0, ML21096A110 |
| [IT-Sys-Crit] | NRC IT System Criticality Tool, ML16064A419 |
| [MD 12.0] | MD 12.0, "Glossary of Security Terms" https://usnrc.sharepoint.com/teams/NRC-Management-Directives/SitePages/MD-12.000.aspx |
| [MD 12.5] | MD 12.5, "NRC Cybersecurity Program" https://usnrc.sharepoint.com/teams/NRC-Management-Directives/SitePages/MD-12.005.aspx |
| [MRF-BIA] | NRC MEF Business Impact Analysis (BIA) Worksheet, ML18318A007 |
| [NRC COOP] | NRC Continuity of Operations Plan, ML14024A688 |
| [NRC ISA] | NRC Information Security Architecture, Version 1.0, July 2, 2021 https://usnrc.sharepoint.com/teams/OCIO-CSO/_layouts/15/viewer.aspx?sourcedoc={96da0157-eb48-444a-a569-7be4c1da2c92} |
| [NRC SP] | NRC Strategic Plan Fiscal Years 2022-2026, NUREG-1614, Vol. 8 https://adamsxt.nrc.gov/navigator/AdamsXT/content/downloadContent.faces?objectStoreName=MainLibrary&vsId={E96C51CE-A511-C502-BB00-7BF426400000}&ForceBrowserDownloadMgrPrompt=false |
| [Risk strategy] | NRC Risk Management Strategy, Revision 1.0, ML20266G443 |
| [SCRM Strategy] | NRC Supply Chain Risk Management Strategy, Revision 1.0, September 2020, ML20177A361 |

# APPENDIX D GLOSSARY

| | |
|---|---|
| Exiger | Supply chain risk service that uses an AI-powered Platform to drive transformational change in how entities are vetted at an unprecedented scale. DDIQ identifies, validates and analyzes global risk indicators by aggregating open source information, performing entity disambiguation, assessing and continuously monitoring ongoing risk to the companies and suppliers within the relevant supply chain network. |
| Exiger Deep Dive | The Exiger Deep Dive is an Enhanced Due Diligence Report, which are reports produced by Exiger's team of analysts and subject matter experts that:<br>• Fully trace back and map ultimate beneficial ownership<br>• Incorporate DDIQ profile data and external data sources covering additional trade data, visa sponsorship information, software vendor and sales networks, cyberhygiene, and cybersecurity evaluations |
| ICT | Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). Source(s): CNSSI 4009-2015 from DoDI 5200.44 |
| ICT Products | Information and communications technology hardware, software, or services. |
| Illumination | Macro/large-scale identification, assessment, and visualization of a program, product, or sectoral supply chain. Utilizes both DDIQ and Exiger Subject Matter Experts to uncover complex risk trends across hundreds or thousands of relevant entities, vendors, contracts, or other links in the targeted supply chain. |
| Level of Supply Chain Risk | The risk is determined to be {Low, Moderate, High, Very High}, where:<br>• Low indicates that NRC has a full understanding and documentation of all supply chain risks, and that understanding includes minimal potential impact to the NRC mission.<br>• Moderate indicates that NRC has some understanding and documentation of supply chain risks that could potentially impact the NRC mission, or NRC has identified supply chain risks that are currently impacting the NRC mission. |

| | |
|---|---|
| | • High indicates that NRC has some understanding and documentation of supply chain risks that could potentially impact the NRC mission, or NRC has identified supply chain risks that are currently impacting the NRC mission significantly.<br><br>• Very High indicates that NRC has almost no understanding and documentation of supply chain risks that could potentially impact the NRC mission. |
| Non-Tier 1 HVAs | Represent systems of significant impact to both the agency and the nation. |
| Privacy Impact Assessment | An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis. |
| SCRA | An NRC created supply chain risk assessment document that identifies an NRC SCR acceptance determination and the rationale supporting the determination. |
| Security Categorization | The determination of the security category for information or an information system. Security categorization methodologies are described in CNSSI 1253 for national security systems and in FIPS 199 for other than national security systems. |
| Tier 1 HVAs | Represent systems of critical impact to both the agency and the nation. |

## <Company Name> Supply Chain Risk Assessment Change History

| Date | Version | Description of Changes | Method Used to Announce & Distribute |
|---|---|---|---|
| <nn-Ddd-yy> | <Ver> | <Description> | <Method> |
| | | | |
| | | | |
| | | | |