

Nuclear Regulatory Commission  
Office of the Chief Information Officer  
Computer Security Process

Office Instruction: **CSO-PROS-0011**

Office Instruction Title: **Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available**

Revision Number: **1.0**

Effective Date: **01-Apr-23**

Primary Contacts: **Kathy Lyons-Burke**  
**Senior Level Advisor for Information Security**

Responsible Organization: **OCIO/CSO**

Summary of Changes: CSO-PROS-0011, "Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available," defines the process that must be used to evaluate NDAA Section 889 compliance when an NDAA Section 889 certification is not available.

ADAMS Accession No.: ML23055A034

Agency Official	Approval Signature and Date
Gar0 Nalabandian Chief Information Security Officer (CISO) Office of the Chief Information Officer (OCIO)	

# Table of Contents

1	Purpose .....	1
2	General Requirements.....	1
3	When Product/Service Being Acquired is Provided by an Identifiable Entity.....	1
3.1	Collect Information from DDIQ Profile .....	2
3.1.1	State Owned Company .....	2
3.1.2	Business with State Owned Enterprise .....	2
3.1.3	Links to Sanctioned Jurisdictions .....	2
3.1.4	Violation Related .....	2
3.1.5	Nationality.....	3
3.2	Collect Information from from Exiger Dashboard .....	3
3.2.1	Company Geographic Locations .....	3
3.2.2	Foreign Risk Breakdown .....	3
3.2.3	Recent China Connected economic activity .....	3
3.2.4	Ownership Target Values .....	3
3.2.5	NDAA Section 889 Mentions .....	3
4	When Product/Service Being Acquired is NOT Provided by an Identifiable Entity .....	3
5	Evaluator NDAA Section 889 Determination .....	4
Appendix A	Acronyms .....	5

# Computer Security Process

## CSO-PROS-0011

Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available

---

### 1 PURPOSE

CSO-PROS-0011, "Supply Chain Evaluation Process for NDAA Section 889 when Certification not Available," defines the process that must be used to evaluate National Defense Authorization Act (NDAA) Section 889 compliance when an NDAA Section 889 certification is not available.

### 2 GENERAL REQUIREMENTS

The NDAA for fiscal year (FY) 2019 prohibits agencies from purchasing telecommunications equipment and services produced or provided by specific entities, including all subsidiaries or affiliates and prohibits the government from doing business with entities that use end products produced by these companies. It also covers the use of any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. All contractors doing or seeking to do business with the NRC must provide a statement of NDAA Section 889 compliance. The [NEAT website](#) provides complete guidance on NDAA Section 889 requirements.

If an Information and Communications Technology (ICT) product or service is not NDAA Section 889 compliant, NRC must **not** acquire the product or service and must stop using any products or services already in use as soon as possible.

In some instances, NRC is unable to obtain an NDAA Section 889 compliance certification from the provider. In those instances where the product or service is needed for NRC to perform its mission, this process is followed to evaluate the risk of NDAA Section 889 non-compliance.

The OCIO Cyber Security Oversight Team (CSOT) representative to the OCIO intake process notifies the CSOT Lead of the need for an NDAA Section 889 evaluation for a product or service.

The CSOT Lead appoints an Evaluator to perform this process.

The Evaluator must check to ensure that the provider is not prohibited ([Trade Adjustment Assistance \(TAA\) Designated Country List](#), [NDAA Section 889](#)) If the provider is prohibited, purchase is not permitted.

### 3 WHEN PRODUCT/SERVICE BEING ACQUIRED IS PROVIDED BY AN IDENTIFIABLE ENTITY

The Evaluator checks to see if an entity profile already exists within the Exiger tool. If so, the Evaluator uses that profile. If not, the Evaluator uses [CSO GUID-7001, "Guide to Generating an Exiger Profile"](#) to generate a Full Profile on the entity providing the product or service.

This process uses both the Exiger DDIQ and the DDIQ analytics dashboard. The Evaluator must login to both websites to obtain the needed information.

Once the data is available in the Exiger dashboard, the Evaluator performs the following actions and captures the data using [CSO-TEMP-0011, "NDAA Section 889 Evaluation Template when Certification not Available"](#) entity NDAA Section 889 evaluation template.

### **3.1 Collect Information from DDIQ Profile**

The evaluator captures the cage code and the entity URL used in the DDIQ profile and places those values into the evaluation template.

The evaluator captures the date the DDIQ profile was run and places that date into the evaluation template.

The evaluator places the product or service name that is being obtained along with the purpose for the product or service in the evaluation template.

The Evaluator uses the following Exiger DDIQ profile sections to collect and evaluate information related to NDAA Section 889.

#### **3.1.1 State Owned Company**

The evaluator examines the references associated with State Owned Company and identifies any information indicating ownership by China. This information is entered into the template associated with ties to China.

#### **3.1.2 Business with State Owned Enterprise**

The evaluator examines the references associated with Business with State Owned Enterprise and identifies any information indicating business with enterprises owned by China. This information is entered into the template associated with ties to China.

#### **3.1.3 Links to Sanctioned Jurisdictions**

The evaluator examines the references associated with Links to Sanctioned Jurisdictions and identifies any information indicating ties to NDAA Section 889 forbidden entities. This information is entered into the template associated with ties to 889 forbidden entities.

#### **3.1.4 Violation Related**

The evaluator examines the references associated with Violation Related and identifies any information indicating ties to China or NDAA Section 889 forbidden entities. This information is entered into the template associated with ties to 889 forbidden entities or ties to China.

### **3.1.5 Nationality**

The evaluator examines the references associated with Nationality and identifies any information indicating ties to China or NDAA Section 889 forbidden entities. This information is entered into the template associated with ties to 889 forbidden entities or ties to China.

## **3.2 Collect Information from from Exiger Dashboard**

The Evaluator uses the following Exiger dashboard sections to collect and evaluate information related to NDAA Section 889.

### **3.2.1 Company Geographic Locations**

The evaluator examines the entity headquarters locations and other locations and identifies any locations that reside within China. This information is entered into the template associated with ties to China.

### **3.2.2 Foreign Risk Breakdown**

The foreign risk breakdown is examined to identify any NDAA Section 889 relevant information. Any information that indicates possible violations of NDAA Section 889 by the entity is noted in the section for ties to NDAA Section 889 forbidden entities.

### **3.2.3 Recent China Connected economic activity**

The evaluator examines the section associated with recent China connected economic activity and enters this information into the section related to ties with China.

### **3.2.4 Ownership Target Values**

The evaluator examines the ownership target values and identifies any locations that reside within China. This information is entered into the template associated with ties to China.

### **3.2.5 NDAA Section 889 Mentions**

The NDAA Section 889 mentions section is examined to identify any NDAA Section 889 relevant information. Any information that indicates possible violations of NDAA Section 889 by the entity is noted in the section for ties to NDAA Section 889 forbidden entities.

## **4 WHEN PRODUCT/SERVICE BEING ACQUIRED IS NOT PROVIDED BY AN IDENTIFIABLE ENTITY**

The Evaluator performs the following steps to identify any indication that acquisition of a product or service violates NDAA Section 889:

- Use the Section 889 Request Bot as described in the [Section 889 Bot Instruction Guide](#) to identify any potential NDAA violation in acquisition of the product or service.
- Perform a Google search that includes the product or service name and the name of a country forbidden by [NDAA Section 889](#). A separate search must be performed using each

country identified. Identify any information that may indicate a violation of NDAA Section 889.

- Perform a Google search that includes the product or service name and the name of a vendor forbidden by [NDAA Section 889](#). A separate search must be performed using each vendor identified. Identify any information that may indicate a violation of NDAA Section 889.
- Perform a Google search that includes the product or service name and the name of a Video Surveillance and Telecommunications Equipment company forbidden by [NDAA Section 889](#). A separate search must be performed using each company identified. Identify any information that may indicate a violation of NDAA Section 889.
- Perform a Google search that includes the product or service name and the name of software forbidden by [NDAA Section 889](#). A separate search must be performed using each software identified. Identify any information that may indicate a violation of NDAA Section 889.
- Identify the product or service home Uniform Resource Locator (URL) and perform a “Who is” lookup to identify where web site is located. Identify any information that may indicate a violation of NDAA Section 889.
- Identify the product or service home URL and perform an Internet Corporation for Assigned Names and Numbers (ICANN) lookup to identify where web site is registered. Identify any information that may indicate a violation of NDAA Section 889.

## 5 EVALUATOR NDAA SECTION 889 DETERMINATION

The Evaluator examines all the NDAA Section 889 relevant information and evaluates whether or not it appears as if obtaining the product or service violates NDAA section 889. This evaluation is provided in the template as the evaluator assessment of NDAA Section requirements for this product or service.

If the Evaluator has concerns about product or service violating NDAA Section 889, the Evaluator provides those concerns to the Cyber Security Oversight Team lead. The Cyber Security Oversight Team lead may sign the evaluation form or may escalate to the CISO. The CISO may sign the evaluation form or may escalate to the Senior Agency Official for Supply Chain Risk Management (SAOSCRM). The SAOSCRM makes the final decision and signs the evaluation form.

The Evaluator applies a digital signature to the form and stores the signed NDAA Section 889 evaluation form in the appropriate area of the [NDAA 889 Cert Info Not in SAM.gov](#) SharePoint site and notifies the requester and the Cyber Security Oversight Team Lead of the availability of the signed form.

## **APPENDIX A    ACRONYMS**

ADAMS	Agencywide Documents Access and Management System
CISO	Chief Information Security Officer
CSO	Computer Security Organization
CSOT	Cyber Security Oversight Team
FY	Fiscal Year
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
NDAA	National Defense Authorization Act
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
SAOSCRM	Senior Agency Official for Supply Chain Risk Management
TAA	Trade Adjustment Assistance
URL	Uniform Resource Locator

### CSO-PROS-0011 CHANGE HISTORY

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
22-Mar-23	1.0	Initial release	SCRM WG Meetings	None needed.