

# SELF-INSPECTION HANDBOOK

## FOR NISP CONTRACTORS





# SELF-INSPECTION HANDBOOK

## FOR NISP CONTRACTORS

### Table of Contents

#### Section 1 - Overview

#### Section 2 - Risk Exposure

#### Section 3 - Inspection Checklists

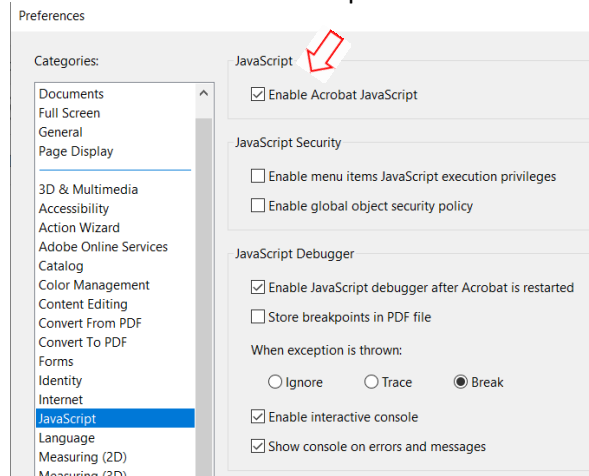
#### Section 4 - Inspection Findings

#### Appendix 1 - Questions for Employees

1) This file should be edited from a local drive, i.e., not from a corporate shared drive or over a VPN connection. The file may be stored on a shared drive.

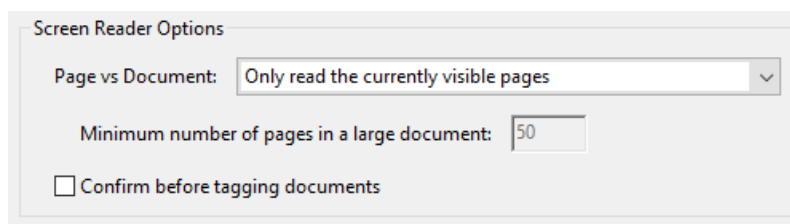
2) For full functionality of controls and summary information enable JavaScript:

- On menu, Click Edit - Preferences - JavaScript. Ensure that JavaScript is enabled



3) To avoid performance issues with scripts advise adjusting reading settings:

- On menu, Click Edit - Preferences - Reading. Choose "Only read the currently..."



## Section 1 - Handbook Overview

### Purpose

This section explains how to use this handbook in support of your self-inspection and provides recommendations for conducting and reporting the results of the self-inspection. For additional information contact your Industrial Security Representative.

### The Self-Inspection Handbook for NISP Contractors

The 32 CFR Part 117 requires all participants in the National Industrial Security Program (NISP) to conduct self-inspections to include an insider threat self-assessment. [32 CFR Part 117.7 (h)(2)(ii)]

This handbook will assist you in complying with these requirements. These checklists are a starting point for establishing and managing an effective self-inspection program tailored to the security needs of your cleared company.

### Purpose of a Self-Inspection

The self-inspection provides insight into the effectiveness of your security program. It enables you to validate that your company's security procedures meet National Industrial Security Operating Manual (NISPOM) requirements and adequately protect national security information, associated assets, and supporting business systems.

As a cleared NISP contractor, you have the responsibility to inspect and monitor the protection of classified information, controlled unclassified information, and key data related to your programs. An effective security program requires an intelligence-led, asset-focused, and threat-driven foundation. A thorough self-inspection is key in the identification of program weaknesses. It will clarify the threats to your facility, security measures in place to mitigate risks, and actions to reduce vulnerability.

This is your chance to take an in-depth look at what your company is doing to protect our national security: to see what is working well and what you may need to change. Remember, you should not be conducting your self-inspection just to meet NISPOM requirements. You should be conducting your self-inspection to ensure the continued protection of our national security, technology, our country, its citizens, and most importantly our military servicemen and servicewomen.

### The Self-Inspection Handbook Structure

Section 1 - Handbook Overview (this section). Provides context and guidance for conducting an effective self-inspection.

Section 2 - Risk Exposure. Provides a set of plain language questions to identify risk exposure and filter handbook for applicable sections.

Section 3 - Inspection Checklists. Contains self-inspection questions grouped by 32 CFR Part 117 sections. Relevant citations provided.

Section 4 - Inspection Findings. Permits documentation of actions taken to remediate inspection findings.

## Relationship between Sections and Recommended Sequence

Read over this section first. In any section, click ⓘ to obtain supplemental information.

Complete Section 2 before Section 3. Section 2 contains responses that will filter Section 3 for applicable content. Section 2 also has additional questions to establish context.

After Section 3 move to Section 4. Use the Import button to create findings for each "No" entry in Section 3. Add other findings or observations relevant to the self-inspection.

## The Elements of Inspection (Checklists)

The self-inspection checklists are arranged according to 32 CFR Part 117. Not all checklists will apply to every cleared company. Complete Section 2 to determine which ones apply to your facility. These are included in Section 3.

There are eight checklists that are common to ALL cleared companies

- Procedures [117.7]
- Reporting Requirements [117.8]
- Entity eligibility determination for access... [117.9]
- (Contractor) eligibility for access to classified... [117.10]
- Foreign Ownership, Control, or Influence (FOCI) [117.11]
- Security training and briefings [117.12]
- Classification [117.13]
- Visits and meetings [117.16]

There are thirteen additional checklists applicable to companies with Safeguarding

- Marking requirements [117.14]
- General safeguarding [117.15(a)]
- Standards for Security Equipment [117.15(b)]
- Storage [117.15(c)]
- Intrusion Detection System (IDS) [117.15(d)]
- Information Controls [117.15(e)]
- Transmission of classified information [117.15(f)]
- Destruction [117.15(g)]
- Disclosure [117.15(h)]
- Disposition [117.15(i)]
- Retention [117.15(j)]
- Termination of security agreement [117.15(k)]
- Safeguarding CUI [117.15(l)]

The remaining checklists apply in special cases and will be included if they relate to your security program. As your program changes (e.g., from a non-possessing to a possessing facility), you will need to revise your self-inspection.

Not all of the questions within each checklist will apply to your program. Review each requirement in the context of your industrial security program. If the requirement applies, your procedures should comply with it and your self-inspection should assess your compliance. Note: In all cases, regulatory guidance takes priority over company-established procedures.

## Self-Inspection Process

To be most effective, it is suggested that you view your self-inspection as a three-step process:

- 1) Pre-inspection
- 2) Inspection
- 3) Post-inspection

### 1) Pre-Inspection

Preparation for the self-inspection begins with your pre-inspection research:

- 1) Identify all security checklists that apply using Section 2 questions.
- 2) Familiarize yourself with how your company's business is organized (it may have an impact on your company's security procedures).
- 3) Identify who you will need to interview and what records you may want to review.
- 4) Schedule meetings in advance to allow participants to prepare.
- 5) Prepare a list of questions and topics that need to be covered.
- 6) Know your facility's physical layout (e.g., where the classified material is stored or where it is worked on).
- 7) Identify the current threats to your company's technologies (contact your assigned counterintelligence special agent, if needed).
- 8) Have a basic knowledge of your company's classified programs.

Remember, your primary sources of information during your self-inspection are people and processes. Take the time to adequately prepare yourself by reviewing the documentation you already have on-hand. This includes the results of your last Defense Counterintelligence and Security Agency (DCSA) security review, security vulnerability assessment, any continuous monitoring (CM) engagements, your current DD Forms 254, "Department of Defense Contract Security Classification Specification," and classification guides, any recent company press releases or publications, your company website, any security records you may have on hand, and the Defense Information System for Security (DISS) records for your cleared employees.

Once you have completed your pre-inspection research, your next step is to set the date to conduct your self-inspection. Once your date is established, meet with your senior management team so they can understand the importance of your self-inspection and provide the support you need to be effective. Additionally, take the time to meet with program and department managers to let them know what support you might need from them during the self-inspection process. Finally, make a formal announcement so that your employees will know what to expect.



## 2) Inspection

The self-inspection process includes gathering information about each of the inspection areas that apply to your company's classified involvement. Your job as the facility security officer (FSO) is to verify and validate that your facility security program is in compliance with applicable NISPOM requirements and that all classified information entrusted to your company is adequately protected.

To do this, review the self-inspection questions against the appropriate documentation (including your classified information) and the people (including their actions) involved in the facility's industrial security program. The self-inspection checklists provide you with the requirements organized by areas of common security concern. These should not be viewed independently during your self-inspection, but interdependently.

During the self-inspection, take the time to explain the self-inspection process and what is expected of each employee you interview. This may be their first time going through any type of inspection and understanding the purpose will enable them to contribute most effectively.

Do not limit yourself to just talking with your employees. Look at their processes, have them demonstrate what they do when working with classified information, spot check documentation, and inspect security equipment to include any Intrusion Detection Systems (IDS), Information Systems (IS), and security containers to which they have access or for which they are responsible.

A quality self-inspection depends on your ability to ask follow-up questions and listen to the answers you receive. This may identify security problems that would otherwise not be brought to your attention. Seek information about current procedures and changes, which could affect future actions. Check security records, test security systems, and most importantly talk to people in their workspaces!

There are certain employees based on position whom you may want to target for interviews during your self-inspection to include your key management personnel, program managers, information technology (IT) personnel, sales personnel, business development personnel, supply chain personnel, human resources personnel, contracts personnel, the receptionist, and mailroom personnel to suggest a few.

### General Interviewing Techniques

- Talk in a conversational tone and maintain eye contact. Let people tell their stories.
- Ask open-ended questions (using who, what, where, when, why, and how).
- Avoid leading questions.
- Let people show you how they perform their jobs to comply with security requirements.
- Follow-up the checklist questions with your own questions.
- Keep good notes for future reference and document corrective actions.

For additional recommendations on specific topics and questions when interviewing employees refer to Appendix 1 - Questions for Employees - click here: [i](#)

### 3) Post-Inspection

Once you have completed your self-inspection, it is critical to take action to correct any problem areas you identified during your self-inspection. You may need to develop additional security education materials to address these problem areas. Key tasks follow:

**Feedback.** It is important to provide immediate feedback to both your management and employees. Significant time and resources were expended to get them vested in this process. Make sure to keep them vested by providing accurate, specific, and clear feedback.

**Recognition.** Make sure to provide “kudos” to any of your employees that were found to have gone above and beyond your established security procedures to ensure the protection of your classified material.

**Reporting.** Finally, in accordance with 32 CFR Part 117 NISPOM Rule, 117.7(h)(2)(ii), you must prepare a formal report describing the self-inspection, its findings, and resolution of issues found. Retain this formal report for DCSA review through the next DCSA security vulnerability assessment. This requirement is supported by Section 4 - Inspection Findings.

**Certification.** In writing and on an annual basis, a Senior Management Official (SMO) at your facility will certify to DCSA, the Cognizant Security Agency (CSA), that a self-inspection has been conducted, senior management has been briefed on the results, appropriate corrective action has been taken, and management fully supports the security program. Record certification in the National Industrial Security System (NISS).

### Technical Notes

#### Navigation

- The Table of Contents is located on page 2.
- Individual pages include a "Top" button to return to the first page of that section.
- The first page of a section includes a "Home" button to return to the originating page.

#### Actions

- Clear. Section 3 checklists and Section 4 findings entries may be cleared using this button. Caution: This is not reversible and all data entered will be permanently deleted.
- Export. Section 3 checklists and Section 4 findings entries may be extracted for export. Clicking this button will prepare associated content in a tab-delimited format for copy-paste extraction into desired application (e.g., MS Excel or Word).
- Import. Section 4 entries may be auto-populated from the "No" entries in Section 3 using this button. Once the finding has been created it may be edited normally in Section 4 as desired. Caution: Any open findings for which there is no longer a "No" entry in Section 3 will be removed. To retain findings for historical reference ensure they are set to "Closed" to prevent removal.
- Close. Sections may be closed using this button. Content will not be affected.

### Changes from Previous Version (from ver 6 to ver 7)

Page (Item)	Change
117.14-3	Page displayed out of order; corrected
117.14-4	Page displayed out of order; corrected
117.17-2	Input fields hidden; corrected

### Changes from Previous Version (from ver 5 to ver 6)

Page (Item)	Change
various	Grammatical edits
117.07-3 (7.006)	Reference corrected from 117.7(c) to 117.7(b)(4)
117.07-3 (7.007)	Reference corrected from 117.7(c) to 117.7(d)
117.07-4 (7.009)	Reference corrected from 117.7(d) to 117.7(e)



## Section 2 - Risk Exposure

### Instructions

This section captures the Risk Exposure of the facility based on your Operational Requirements and Business Practices. Check the statements that are applicable.

*Note: Items with Sec #s used to select checklists needed for your self-inspection.*

### Operational Requirements Exposure

- ☐ My facility controls physical locations where work on government contracts or research is performed
- ☐ My facility has systems or networks with information related to government contracts or research
- ☐ My facility has operational requirements for FOCI Mitigation
- ☐ My facility has a contractual requirement for safeguarding (Secs 117.14, 15)
- ☐ My facility has classified subcontracts in support of classified contracts (Sec 117.17)
- ☐ My facility has Classified Information Systems (Sec 117.18)
- ☐ My facility has contractual requirements for international operations (Sec 117.19)
- ☐ My facility has contractual requirements for Critical Nuclear Weapon Design Information (CNWDI) (Sec 117.20)
- ☐ My facility has contractual requirements for COMSEC (Sec 117.21)
- ☐ My facility has contractual requirements for OPSEC
- ☐ My facility has contractual requirements for TEMPEST

### Business Practices Exposure

- ☐ My facility uses cleared consultants (Sec 117.9)
- ☐ My facility is reliant on products, systems, or services provided by external suppliers to carry out missions and business functions (exclude commodity suppliers)
- ☐ My facility conducts or supports foreign military or commercial sales
- ☐ My facility conducts meetings / hosts visitors including service providers, maintenance personnel, and/or vendors (Sec 117.16)
- ☐ My facility employs non-U.S. citizens who are physically located where government contracts or research is performed
- ☐ Employees conduct overseas business travel on behalf of my facility or individually
- ☐ Employees attend or participate in conferences, conventions or trade shows, on behalf of my facility or individually

## Section 3 - Inspection Checklists

### Instructions

Checklists have been filtered based on the statements selected in Section 2. Open buttons are displayed for all checklists that apply. Click the Open button to address the questions for each element.

Yes	No	NA	Not Ans	Basic (These apply to all facilities)	
0	0	0	13	<a href="#">Open</a>	<b>Procedures [117.7]</b>
0	0	0	19	<a href="#">Open</a>	<b>Reporting Requirements [117.8]</b>
0	0	0	6	<a href="#">Open</a>	<b>Entity eligibility determination for access... [117.9]</b>
0	0	0	11	<a href="#">Open</a>	<b>(Contractor) eligibility for access to classified... [117.10]</b>
0	0	0	8	<a href="#">Open</a>	<b>Foreign Ownership, Control, or Influence (FOCI) [117.11]</b>
0	0	0	10	<a href="#">Open</a>	<b>Security training and briefings [117.12]</b>
0	0	0	7	<a href="#">Open</a>	<b>Classification [117.13]</b>
				<a href="#">Open</a>	<b>Visits and meetings [117.16]</b>

### Safeguarding

**Marking requirements [117.14]**  
**General safeguarding [117.15(a)]**  
**Standards for Security Equipment [117.15(b)]**  
**Storage [117.15(c)]**  
**Intrusion Detection System (IDS) [117.15(d)]**  
**Information Controls [117.15(e)]**  
**Transmission of classified information [117.15(f)]**  
**Destruction [117.15(g)]**  
**Disclosure [117.15(h)]**  
**Disposition [117.15(i)]**  
**Retention [117.15(j)]**  
**Termination of security agreement [117.15(k)]**  
**Safeguarding CUI [117.15(l)]**

**Subcontracting [117.17]**

**Information system security [117.18]**

**International security requirements [117.19]**

**Critical Nuclear Weapon Design Info... [117.20]**

**COMSEC [117.21]**

Totals	0	0	0	88
--------	---	---	---	----

[Close](#)[Clear](#)[Export](#)**Total Items:** 13**Answered: Yes** 0**No** 0**NA** 0**Not Answered** 13**117.07 - Procedures**

Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

**Program Design**

The comprehensiveness and maturity of the process, people, and tools in your security program



Initial steps;  
not systematic  
yet



Basic program;  
early stages of  
deployment



Solid program;  
some minor  
weaknesses



Well above  
average  
program



Superb  
benchmark  
program

**Program Results**

The effectiveness of your program in providing protection



Limited  
protection  
offered



Basic  
protection in  
key areas



Adequate  
protection in all  
areas




Robust  
protection  
across all  
areas



Superb  
benchmark  
program

Sec 117.07 Procedures					
ID	32 CFR Ref:	Question:	YES	NO	N/A
7.001	117.7(b)(2)	Is the Senior Management Official (SMO) directing the facility's operations and actions necessary for the safeguarding of classified information in the facility or where employees reside at other cleared contractor sites or USG locations?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			
7.002	117.7(b)(2)(ii)	Has the SMO, appointed a contractor employee or employees, in writing as the facility security officer (FSO) and appoint the same employee or a different employee as the Insider Threat Program senior official (ITPSO)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			
7.003	117.7(b)(2)(iii)	Is the SMO fully informed of the facility's classified operations?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			
7.004	117.7(b)(2)(iv)	Is the SMO making decisions based on classified threat reporting and their thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			

Sec 117.07 Procedures					
ID	32 CFR Ref:	Question:	YES	NO	N/A
7.005	117.7(b)(2)(v)	Is the SMO retaining accountability for the management and operations of the facility without delegating that accountability to a subordinate manager?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
7.006	117.7(b)(4)	Does your ITPSO ensure compliance with insider threat requirements established in implementing guidance provided by DCSA?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
7.007	117.7(d)	Does your company have procedures to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
7.008	117.7(e)	Does your company have a Standard Practice Procedures (SPP)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Sec 117.07 Procedures					
ID	32 CFR Ref:	Question:	YES	NO	N/A
7.009	117.7(e)	If your company has an SPP in place, is it current, available to employees, and does it adequately implement the requirements of the 32 CFR Part 117 NISPOM?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
7.010	117.7(d) 117.16(a)(3)	Has the company developed and implemented an Insider Threat Program plan endorsed by the SMO?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
7.011	117.7(d)	Do you have a written Insider Threat Program plan that has been self-certified to DCSA as current and implemented?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
7.012	117.7(e) 117.16(a)(3)	Do you cooperate with Federal agencies and their officially credentialed U.S. Government or contractor representatives during official reviews and investigations concerning the protection of classified information?  	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			



Sec 117.07 Procedures					
ID	32 CFR Ref:	Question:	YES	NO	N/A
7.013	117.7(j)	Is the company advertising the applicable Defense Hotline numbers?  <div>i</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

<b>Total Items:</b> 19	<b>Answered: Yes</b> 0	<b>No</b> 0	<b>NA</b> 0	<b>Not Answered</b> 19
------------------------	------------------------	-------------	-------------	------------------------

**117.08 - Reporting Requirements**

Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

**Program Design**

The comprehensiveness and maturity of the process, people, and tools in your security program

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Initial steps; not systematic yet	Basic program; early stages of deployment	Solid program; some minor weaknesses	Well above average program	Superb benchmark program



**Program Results**

The effectiveness of your program in providing protection

<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Limited protection offered	Basic protection in key areas	Adequate protection in all areas	Robust protection across all areas	Superb benchmark program

117.08 - Reporting Requirements					
ID	32 CFR Ref:	Question:	YES	NO	N/A
8.001	117.8(a) 117.8(d)	Are cleared employees aware of their responsibilities and is the facility reporting in accordance with the requirements of Security Executive Agent Directive 3 (SEAD 3)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.002	117.8(a)(1) 117.8(a)(2)	Are there established internal procedures that ensure cleared employees are aware of their responsibilities for reporting pertinent information to the FSO as required?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.003	117.8(a)(1)	Does your company have reporting procedures for employees, supervisors, or other organizational components to refer relevant insider threat information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.004	117.8(a)(1)	Does the Insider Threat Program have procedures for clarifying, resolving, and reporting potential insider threat matters as appropriate?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

117.08 - Reporting Requirements					
ID	32 CFR Ref:	Question:	YES	NO	N/A
8.005	117.8(a)(1)	Do Insider Threat Program personnel receive regular, timely access to all relevant and credible information to identify violations, areas of concern, or potential insider threat matters? How is the information provided (manually or electronically)?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			
8.006	117.8(b) through 117.8(c)(14)	Does the company have an effective process in place for submission of required reports to the Federal Bureau of Investigation (FBI) and to DCSA?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			
8.007	1117.8(b)	Are reports that are brought to the facilities attention that concern actual, probable, or possible espionage, sabotage, terrorism, or subversive activities reported to the FBI?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			
8.008	117.8(c)	Have reports been submitted to the Vetting Risk Operations Center (VROC) or to DCSA as required? NOTE: CSA designated systems of record may be used for submission of some of these reports.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b>			

117.08 - Reporting Requirements					
ID	32 CFR Ref:	Question:	YES	NO	N/A
8.009	117.8(c)(1) 117.8(c)(2)	Are actions taken to address insider threat review findings in a timely manner?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.010	117.8(c)(1)	Have you reviewed and submitted all adverse information reports received since the last DCSA security vulnerability assessment?  	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.011	117.8(c)(2)	Have you submitted all suspicious contact reports as required? (see Security Executive Agent Directive (SEAD) 3, for specific information to be reported)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.012	117.8(c)(3)	Have all changes in the status of cleared employees been properly reported through the CSA designated system?  	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Section 117.08- Reporting Requirements					
ID	32 CFR Ref:	Question:	YES	NO	N/A
8.013	117.8(c)(5) 117.8(c)(6) 117.10(g)(4)	Have all instances in which an employee refused to be processed for a security clearance or refused to sign the SF 312, "Classified Information Non-disclosure Agreement," been reported through the CSA designated system? Answer NA if no refusals.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.014	117.8(c)(7)(iii) (B)	Has the facility properly implemented exclusion resolutions in place for KMP? Answer NA if no resolutions.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.015	117.8(c)(7)(v)	Have changes to the information previously provided on the facilities SF 328, "Certificate Pertaining to Foreign Interests," been properly reported to DCSA through the CSA designated system?" Answer NA if no changes. <span style="float: right;">(i)</span>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.016	117.8(c)(8)	Have changes in storage requirement or capability to safeguard classified material been properly reported? Answer NA if no changes.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			



117.08 - Reporting Requirements					
ID	32 CFR Ref:	Question:	YES	NO	N/A
8.017	117.8(d)	Are all employees (cleared and uncleared) aware of what constitutes a security violation and to whom it should be reported?  <div style="text-align: right;">(i)</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.018	117.8(e)(2)	Is there a graduated scale of administrative disciplinary action that is applied against employees who violate requirements of the NISPOM?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
8.019	117.8(f)(1)	Do you have a process in place to report all cyber intrusions to the designated DoD CSO ?  <div style="text-align: right;">(i)</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

Total Items: 6      Answered: Yes 0      No 0      NA 0      Not Answered 6

**117.09 - Entity eligibility determination for access...**

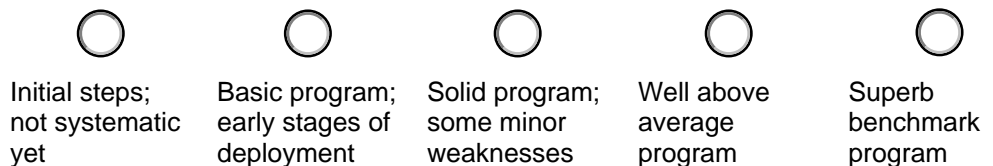
Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

Program Design

The comprehensiveness and maturity of the process, people, and tools in your security program





Program Results

The effectiveness of your program in providing protection



Sec 117.09 - Entity eligibility determination for access...					
ID	32 CFR Ref:	Question:	YES	NO	N/A
9.001	117.9(a)	Is the facility clearance and safeguarding capability of the receiving facility verified prior to transmission of classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
9.002	117.9(a)(9)	Have you verified that the company's entity eligibility has not been used for advertising or promotional purposes?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
9.003	117.9(d)(1)(v)	Are the SMO, the ITPSO, the FSO, and, if required by DCSA, other KMP cleared in connection with the FCL?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
9.004	117.9(f)	Have the proper exclusion actions been executed for uncleared company officials and furnished to the Cognizant Security Agency (CSA)?  <div style="text-align: right;"> <input type="radio"/> <input type="radio"/> <input type="radio"/> </div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Sec 117.09 - Entity eligibility determination for access...					
ID	32 CFR Ref:	Question:	YES	NO	N/A
9.005	117.9(i)	Does the home office have an entity eligibility at the same level as the highest entity eligibility determination within the multiple facility organization?  	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
9.006	117.9(p)	Are the original CSA designated forms (DD Form 441, "Department of Defense Security Agreement," and SF 328, "Certificate Pertaining to Foreign Interests") available, properly executed, and current?  	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

Total Items: 11      Answered: Yes 0      No 0      NA 0      Not Answered 11

**117.10 - (Contractor) eligibility for access to classified...**

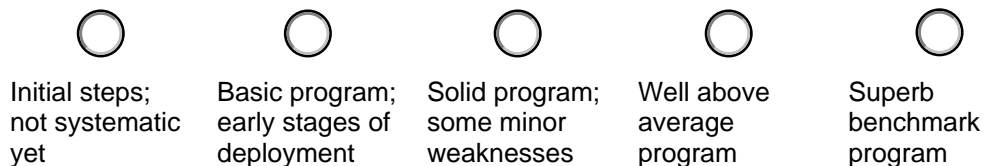
Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

Program Design

The comprehensiveness and maturity of the process, people, and tools in your security program



Program Results

The effectiveness of your program in providing protection



Sec 117.10 - Determination of eligibility for access...					
ID	32 CFR Ref:	Question:	YES	NO	N/A
10.001	117.10(a)(1)	Have personnel with a contractual requirement to access classified information been granted access at the required level?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.002	117.10(a)(3)	Is all the information in the CSA designated personnel security system pertaining to your cleared employees accurate and up to date?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.003	117.10(a)(3)	Does each employee's record in the CSA designated personnel security system indicate an appropriate "eligibility" and "access?"	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.004	117.10(a)(3)	Have all users and account managers been officially appointed, issued unique usernames and passwords, public key infrastructure credentials or equivalent, and given the appropriate level of access in the CSA designated personnel security system?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			



Sec 117.10 - Determination of eligibility for access...					
ID	32 CFR Ref:	Question:	YES	NO	N/A
10.005	117.10(a)(3) 117.12(c)	Have all users of the CSA designated personnel security system received appropriate training for their responsibilities?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.006	117.10(a)(5)	Are the numbers of requests for eligibility for access to classified information held to a minimum, necessary for operational efficiency in accordance with contractual obligations, and consistent with contractual requirements?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.007	117.10(c)	Has citizenship been verified for each applicant for determination of eligibility for access to classified information, using the required documentation?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<div style="text-align: right;">(i)</div> <b>How Implemented/Notes:</b> <div></div>			
10.008	117.10(d)(1) 117.10(d)(2)	Are employees in process for security clearances notified in writing that review of the SF 86, "Questionnaire for National Security Positions," or Electronic Questionnaires for Investigations Processing is for accuracy and completeness only and that the information will not be used for other purposes within the company?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Sec 117.10 - Determination of eligibility for access...					
ID	32 CFR Ref:	Question:	YES	NO	N/A
10.009	117.10(e)	Are procedures in place to ensure the applicant's electronic fingerprints are authentic, legible, and complete to avoid clearance processing delays?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.010	117.10(f)(2)	Are all pre-employment offers based on acceptance to begin employment within 45 days of granting eligibility for access to classified information <span style="float: right;">(i)</span>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
10.011	117.10(g)(1) 117.10(g)(3)	Are Standard Forms 312, "Classified Information Nondisclosure Agreement," properly executed by newly cleared employees prior to accessing classified information and uploaded into the CSA designated system for retention?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

<b>Total Items:</b> 8	<b>Answered: Yes</b> 0	<b>No</b> 0	<b>NA</b> 0	<b>Not Answered</b> 8
-----------------------	------------------------	-------------	-------------	-----------------------

**117.11 - Foreign Ownership, Control, or Influence (FOCI)**

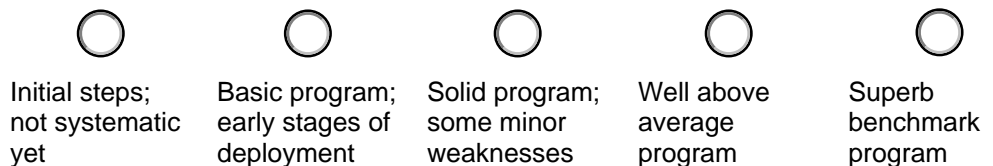
Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

**Program Design**

The comprehensiveness and maturity of the process, people, and tools in your security program


**Program Results**

The effectiveness of your program in providing protection



Sec 117.11 - Foreign Ownership, Control, or Influence (FOCI)					
ID	32 CFR Ref:	Question:	YES	NO	N/A
11.001	117.11(c)	Have all changes in any of the information previously reported on your SF 328 been properly reported to DCSA?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
11.002	117.11(c)(2)	Have you notified DCSA of any negotiations for a merger, acquisition, or takeover by a foreign interest?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
11.003	117.11(d)	If necessary, has a FOCI action plan with all requisite supplements, e.g., Technology Control Plan (TCP), Affiliated Operations Plan (AOP), Electronic Communications Plan (ECP), been submitted to DCSA?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
11.004	117.11(d)(2)(iii)(A)	If cleared under a Special Security Agreement (SSA), has your company received a National Interest Determination (NID) for access to proscribed information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Sec 117.11 - Foreign Ownership, Control, or Influence (FOCI)					
ID	32 CFR Ref:	Question:	YES	NO	N/A
11.005	117.11(g)	If operating under a Voting Trust, Proxy Agreement, SSA, or Security Control Agreement (SCA) has a Government Security Committee (GSC) been appointed by the Board of Directors?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
11.006	117.11(h)(1)	Has a TCP been developed by you, approved by DCSA, and effectively implemented as required under a FOCI action plan or otherwise directed by DCSA?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
11.007	117.11(i)(1)	If operating under a Voting Trust, Proxy Agreement, SSA, or SCA, does the GSC meet annually with DCSA to review the effectiveness of the arrangement?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
11.008	117.11(i)(2)	Is an annual Implementation and Compliance Report submitted by the chairman of the GSC to DCSA as required by the FOCI action plan?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

Total Items: 10

Answered: Yes 0

No 0

NA 0

Not Answered 10

**117.12 - Security training and briefings**

Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

**Program Design**

The comprehensiveness and maturity of the process, people, and tools in your security program



Initial steps; not systematic yet



Basic program; early stages of deployment



Solid program; some minor weaknesses



Well above average program



Superb benchmark program

**Program Results**

The effectiveness of your program in providing protection



Limited protection offered



Basic protection in key areas



Adequate protection in all areas



Robust protection across all areas



Superb benchmark program



Sec 117.12 - Security training and briefings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
12.001	117.12(a)	Are all cleared employees provided with additional security training and briefings commensurate with their involvement with classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.002	117.12(c) 117.20(b) 117.21(e)(1) 117.19(g)(7)	Have you, as the FSO, received initial security briefings, special security briefings, and debriefings provided by DCSA or GCA when required?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.003	117.12(d)	Have you, as the FSO, and others performing security functions, completed training considered appropriate by DCSA as the CSA within 6 months of appointment?  <div style="text-align: right;">(i)</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.004	117.12(e) through 117.12(k)	Do all cleared persons (including those at other locations and temporary help suppliers) receive all initial required security training and every 12 months thereafter?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Sec 117.12 - Security training and briefings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
12.005	117.12(e)	Do initial security briefings contain all required information and is this training administered prior to access to classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.006	117.12(g)	Are the ITPSO and personnel performing duties related to insider threat program management trained in accordance with guidance provided by DCSA?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.007	117.12(h)(1)	Do employees receive appropriate training before they are authorized to make derivative classification decisions for your company?  <div style="text-align: right;">(i)</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.008	117.12(h)(2)	Are employees receiving derivative classification refresher training at the prescribed intervals?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Sec 117.12 - Security training and briefings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
12.009	117.12(k) 117.7(f)	Have all cleared employees completed security refresher training as required?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
12.010	117.12(l)	Are cleared employees debriefed at the time of termination of employment (discharge, resignation, or retirement); when an employee's personnel clearance is terminated, suspended, or revoked; or upon termination of the FCL?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

<b>Total Items:</b> 7	<b>Answered: Yes</b> 0	<b>No</b> 0	<b>NA</b> 0	<b>Not Answered</b> 7
-----------------------	------------------------	-------------	-------------	-----------------------

**117.13 - Classification**

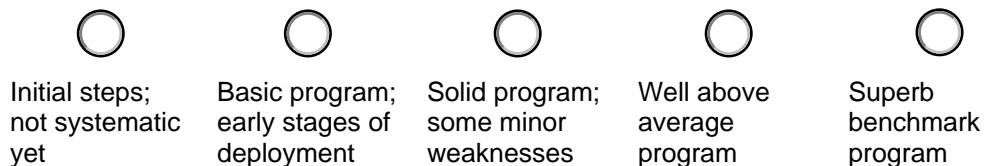
Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

**Program Design**

The comprehensiveness and maturity of the process, people, and tools in your security program

**Program Results**

The effectiveness of your program in providing protection



Section 117.13 - Classification					
ID	32 CFR Ref:	Question:	YES	NO	N/A
13.001	117.13(b)(1)	Is all derivatively classified material appropriately marked?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
13.002	117.13(c)	Are derivative classifiers identified by name and position or by personal identifier on the documents on which they made derivative classification decisions?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
13.003	117.13(d)	Is all classification guidance adequate and is the DD Form 254, "Contract Security Classification Specification," provided as required?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
13.004	117.13(d)(4)(iii)	Do you possess a DD Form 254 for every classified contract issued to your company?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Section 117.13 - Classification					
ID	32 CFR Ref:	Question:	YES	NO	N/A
13.005	117.13(d)(5)	Upon completion of a classified contract has the contractor returned all U.S. Government provided or deliverable information to the custody of the government?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
13.006	117.13(e)	Has the contractor challenged improper or inadequate classification guidance?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
13.007	117.13(f)	Is any contractor-developed information, not supporting the performance of a classified contract (e.g., unsolicited proposals or research products) appropriately classified, marked, and protected?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Close

Clear

Export

Total Items: 14

Answered: Yes 0

No 0

NA 0

Not Answered 14

**117.16 - Visits and meetings**

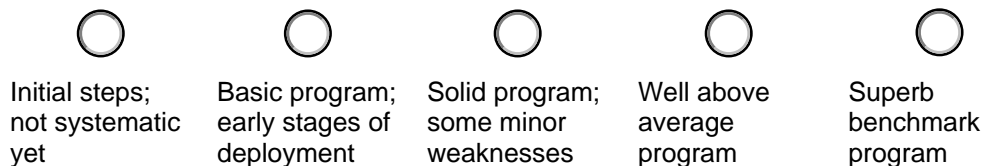
Describe the findings from your most recent self-inspection or DCSA security review in this area.

Describe the actions you have taken and/or will take to mitigate vulnerabilities or improve your security program in this area.

Use the scales below to indicate the overall strength of your security program in this area.

**Program Design**

The comprehensiveness and maturity of the process, people, and tools in your security program

**Program Results**

The effectiveness of your program in providing protection



Section 117.16 - Visits and meetings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
16.001	117.16(a)(1)	Are classified visits held to a minimum?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.002	117.16(a)(1)(ii)	Are procedures established to ensure positive identification of visitors prior to disclosure of classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.003	117.16(a)(1)(iii)	Are procedures established to ensure that visitors are only afforded access to classified information consistent with their visit?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.004	117.16(a)(2)	Is disclosure of classified information based on need to know (a contractual relationship) or an assessment that the receiving contractor has a bona fide need to access classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			



Section 117.16 - Visits and meetings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
16.005	117.16(a)(4)	Are visit authorization requests sent and received through the CSA designated system whenever possible?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		(i) (i)			
<b>How Implemented/Notes:</b> <div style="background-color: #f0f0f0; height: 60px; margin-top: 5px;"></div>					
16.006	117.16(a)(4)(ii)	Do visit authorization requests include the required information and are they updated to reflect changes in the status of that information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>How Implemented/Notes:</b> <div style="background-color: #f0f0f0; height: 60px; margin-top: 5px;"></div>					
16.007	117.16(a)(5)	Are long-term visitors governed by the security procedures of the host contractor?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>How Implemented/Notes:</b> <div style="background-color: #f0f0f0; height: 60px; margin-top: 5px;"></div>					
16.008	117.16(b)(1)	Has the government agency sponsoring the meeting approved all security arrangements, announcements, attendees, and the meeting location?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		(i) (i)			
<b>How Implemented/Notes:</b> <div style="background-color: #f0f0f0; height: 60px; margin-top: 5px;"></div>					

Section 117.16 - Visits and meetings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
16.009	117.16(b)(2)	Did your request for authorization include all required information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.010	117.16(b)(4)(i)	Have all security arrangements been approved by the authorizing agency?  <div style="text-align: right;">(i) (i)</div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.011	117.16(b)(4)(ii)	Is attendance limited to persons appropriately cleared who have the need-to-know?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.012	117.16(b)(5)	Is prior written authorization obtained from the relevant GCA before disclosure of classified information?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

Section 117.16 - Visits and meetings					
ID	32 CFR Ref:	Question:	YES	NO	N/A
16.013	117.16(b)(5)(ii)	Has a copy of the disclosure authorization been furnished to the Government Agency sponsoring the meeting?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			
16.014	117.16(b)(6)	Are your employees properly using the visit request process to obtain approval to attend classified meetings?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		<b>How Implemented/Notes:</b> <div></div>			

## Suggested Questions when Interviewing Uncleared Employees

### **CUI**

- What is Controlled Unclassified Information (CUI)?
- Why is CUI important?
- How does CUI relate to your position?

### **Classified Information**

- What is classified information?
- How would you know if something was classified?
- If you found unprotected classified information what would you do?
- Have you ever heard classified information being discussed?
- Have you ever come into possession of classified materials? How?

## Suggested Questions when Interviewing Cleared Employees

### **Cleared Roles and Responsibilities**

- What is your job title/responsibility?
- What is the level of your security clearance? How long have you been cleared?
- Why are you cleared (describe the contract or programs that require you to be cleared)?
- If recently cleared, what were the processes/steps in applying for your security clearance?

### **Training and General Knowledge**

- When was your last security briefing? What do you recall from that briefing?
- Can you recall any of the following topics being addressed in briefings? Risk Management, Job Specific Security Brief, Public Release, Safeguarding Responsibilities, Adverse Information, Cybersecurity, Counterintelligence Awareness, Insider Threat

### **Access to Classified Information**

- When was your last access to classified information and at what level?
- Have you ever accessed classified information outside of this facility?
- Do you have the combination to any storage containers, access to any closed areas, etc.?
- What are the security requirements regarding combinations to security containers?
- Who, other than yourself, has access to these containers?
- How do you keep track or maintain your knowledge of the combination?
- Is a record maintained of the safe combination? If so, where?

## Suggested Questions when Interviewing Cleared Employees (cont)

### Protection

- Where do you typically work on classified information?
- What procedures do you follow to protect classified information while working on it?

### CUI

- What is Controlled Unclassified Information (CUI)?
- Why is CUI important?
- How does CUI relate to your position?

### Visit Support

- What are the procedure for visitors coming here for a classified visit?
- What are the procedures for individuals going on classified visits?
- What are the procedures to debrief individuals returning from classified visits?
- What are the procedures for securing classified information brought back to the facility?
- What are the procedures for determining need-to-know and giving visitors access to classified information?

### Contacts

- Have you ever been approached by anyone requesting classified information?
- Do you ever work overtime and access classified information?
- What is meant by the term adverse information and how would you report it?
- Can you recall any other reportable items?
- What is an insider threat?
- What are some indicators of insider threat behavior and who would you report this to?
- Can you recall any methods used to recruit trusted insiders?

### Reporting

- What is meant by the term "suspicious contact" and how would you report one?
- Have you ever been cited for a security violation, infraction, or incident?
- What would you do if you committed a security violation, infraction, or discovered one?

## Suggested Questions when Interviewing Cleared Employees (cont)

### Classification Responsibilities

- Do you generate or derivatively classify information? Tell me about it.
- What security controls are established?
- How do you know it's classified?
- Describe the training you received prior to derivatively classifying or generating classified information.
- What do you do with classified information?
- Do you ever use a computer to generate classified information?
- How do you mark this information?
- What information or references do you use when classifying information?
- Please produce the classification guidance that you used. Is it accurate?
- What would you do if you determined that the classification guidance was not accurate?
- What are the security procedures for publishing classified material?

### Note

In addition to asking questions, it is a good idea to ask cleared employees to demonstrate how they perform their security-related tasks, e.g.,

“Show me what you do before processing classified information on your computer” or  
“Show me how you prepare a package for shipment.”

This will allow you not only to verify what the correct procedures are, but to ensure those procedures are being carried out and that classified information is being protected.

[Close](#)[Import](#)[Clear](#)[Export](#)

## Section 4 - Inspection Findings

### Instructions

Provide a record of issues identified during self-inspection and remediation actions.  
Ref: 32 CFR Part 117.7 (h)(2)(ii) Note: certification by FSO is recorded in NISS.

### Guidance

Use "Import Findings" to auto generate findings for all "No" checklist answers. Repeat to update listing. Open findings whose checklist response changes from No to Yes/NA will be removed on update. Change status to "Closed" to retain for historical record. Directly enter any other findings or observations below. Indicate source(s) of non-32 CFR refs.

Issue #	Type	Status	Question ID	32 CFR Ref (or as stated)
001	Choose	Choose	Direct Entry	
Finding/Observation				
Resolution				

Issue #	Type	Status	Question ID	32 CFR Ref (or as stated)
002	Choose	Choose	Direct Entry	
Finding/Observation				
Resolution				

Issue #	Type	Status	Question ID	32 CFR Ref (or as stated)
003	Choose	Choose	Direct Entry	
Finding/Observation				
Resolution				

[Add Page](#)