# DCSA Industrial Self-Inspection Debrief to KMP/SMO

*To: <SMO/KMP Name>*

*From: <FSO/A-FSO Names>*

*Date: <day, month, year>*

|  |  |
| --- | --- |
| **Location** | *<CAGE code>; <address>* |
| **Facility Clearance Status** | *<FCL>* |
| **Inspection Start** | *<date>* |
| **Inspection Completion** | *<date>* |
| **Self-Assessment Rating** |  |
| **Participants** |  |
| **Submitted to** | *<KMP Name> <SMO name> <other stakeholders names>* |

## Purpose

The 32 CFR Part 117 requires all participants in the National Industrial Security Program (NISP) to conduct self-inspections. [32 CFR Part 117.7 (h)(2)(ii)] The self-inspection provides insight into the effectiveness of the *<COMPANY’S>* security program. It enables us to validate that our 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, we have the responsibility to inspect and monitor the protection of classified information, control unclassified information, and control key data related to our programs. An effective security program requires ongoing risk assessments and mitigation that are asset-focused and have a threat-driven foundation. A thorough self-inspection is key in the identification of program weaknesses. It will clarify the threats to our facility, security measures in place to mitigate risks, and actions to reduce vulnerability.

The following provides a review of our policies, procedures, and practices in support of protecting national security. We evaluate what is working well and what we may need to change and/or adapt to continuously improve our practices. A bi-annual self-inspection ensures the continued protection of our national security, technology, our country, its citizens, and the US military.

Table of Contents

[DCSA Industrial Self-Inspection Debrief to KMP/SMO 1](#_Toc122438368)

[Purpose 1](#_Toc122438369)

[Areas for Improvement 4](#_Toc122438370)

[Incidents, Violations, Administrative Findings 4](#_Toc122438371)

[Document Control 4](#_Toc122438372)

[Visits and Meetings 4](#_Toc122438373)

[Reporting Requirements (SEAD-3) 4](#_Toc122438374)

[DCSA Industrial Checklist Report 5](#_Toc122438375)

[Basic Areas 5](#_Toc122438376)

[Procedures [32 CFR Part 117, Section 7; 117.7] 5](#_Toc122438377)

[Incidents, Violations, Administrative Findings 5](#_Toc122438378)

[Senior Management Official (SMO) 5](#_Toc122438379)

[Insider Threat Program 5](#_Toc122438380)

[Standard Practice Procedures (SPP) 5](#_Toc122438381)

[Visiting Government Investigators & Industrial Security Representatives (ISR) 5](#_Toc122438382)

[Reporting Requirements [117.8] 5](#_Toc122438383)

[Entity Eligibility Determination for Access [117.9] 5](#_Toc122438384)

[Contractor Eligibility for Access to Classified [117.10] 5](#_Toc122438385)

[Foreign Ownership, Control, or Influence [FOCI] [117.11] 5](#_Toc122438386)

[Security Training and Briefings [117.12] 5](#_Toc122438387)

[Classification [117.13] 5](#_Toc122438388)

[Visits and Meetings [117.16] 5](#_Toc122438389)

[Safeguarding 5](#_Toc122438390)

[Marking Requirements [117.14] 5](#_Toc122438391)

[General Safeguarding [117.15(a)] 5](#_Toc122438392)

[Standards for Security Equipment [117.15(b)] 6](#_Toc122438393)

[Storage [117.15(c)] 6](#_Toc122438394)

[Intrusion Detection System (IDS) [117.15(d)] 6](#_Toc122438395)

[Information Controls [117.15(e)] 6](#_Toc122438396)

[Transmission of Classified Information [117.15(f)] 6](#_Toc122438397)

[Destruction [117.15(g)] 6](#_Toc122438398)

[Disclosure [117.15(h)] 6](#_Toc122438399)

[Disposition [117.15(i)] 6](#_Toc122438400)

[Retention [117.15 (j)] 6](#_Toc122438401)

[Termination of Security Agreement [117.15(k)] 6](#_Toc122438402)

[Other Areas 6](#_Toc122438403)

[Safeguarding CUI [117.15(l)] 6](#_Toc122438404)

[Subcontracting [117.17] 6](#_Toc122438405)

[Information Security Systems [117.18] 6](#_Toc122438406)

[COMSEC [117.21] 6](#_Toc122438407)

## Areas for Improvement

*<In this section, summarize areas for improvement across the security program. Examples of common areas for findings are below.>*

### Incidents, Violations, Administrative Findings

*<list mitigation steps taken or recommendations for improving if issues aren’t zero>*

### Document Control

*<note the common areas of concern like headers/footers, presence of industry classification authority blocks, addresses, copies of originals, copies of copies, etc.>*

### Visits and Meetings

*<note any issues w/ the receiving of clearances, hosting foreign nationals, sanitizing rooms, etc.>*

### Reporting Requirements (SEAD-3)

*<DCSA is very interested in self-reporting metrics and getting those reports forwarded to them. Note areas to improve the reporting frequency through training and/or general staff awareness.>*

# DCSA Industrial Checklist Report

*NOTE: This checklist is formatted from the relevant sections of the NISP Checklist. Your audience is your company SMO/KMP/other relevant stakeholders. The information reported here should be transparent, honest, and clear; and should include a summary of all findings* ***since your last self-inspection****.*

## Basic Areas

#### Procedures [32 CFR Part 117, Section 7; 117.7]

##### Incidents, Violations, Administrative Findings

##### Senior Management Official (SMO)

##### Insider Threat Program

##### Standard Practice Procedures (SPP)

##### Visiting Government Investigators & Industrial Security Representatives (ISR)

#### 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]

### 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)]

### Other Areas

#### Safeguarding CUI [117.15(l)]

#### Subcontracting [117.17]

#### Information Security Systems [117.18]

#### COMSEC [117.21]