



L3HARRIS

FAST. FORWARD.

CONTRACTOR SELF- INSPECTIONS

Requirements, Best Practices

Thomas Krell – L3Harris Technologies, Inc.

FISWG/NCMS 2022

Agenda



- Self-Inspection Purpose
- Self-Inspection Policy Requirements
- Self-Inspection Objectives
- DCSA Self-Inspection Handbook (SIH)
- Self-Inspection Process
- Self-Inspection Products/Tips

Self-Inspection Purpose



- The self-inspection provides insight into the effectiveness of your security program
- It enables you to validate that your company's security procedures meet 32 CFR requirements and adequately protects national security information
- **A thorough “DCSA Style” self-inspection is key in the identification of program weaknesses - no conference room inspections, check, verify, annotate**
- Your self-inspection results evaluate security measures in place to reduce risk and actions to reduce vulnerability
- The results are further enhanced by considering threat information relevant to the NISP, or more specific to the products or services you provide to the government, and the technologies and programs they involve
- The self-inspection is a key tool in ensuring your facility is well-prepared for a DCSA security review
- Proactive communication of the results of your review with your ISR (and ISSP, if applicable) ensure comprehensive mitigation to issues, as well as valuable feedback on the effective implementation of best practices

Self-Inspection Policy Requirements



- 32 CFR Part 117.7 Procedures. (h) Security reviews.
- (2) Contractor reviews. Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.
 - (i) Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspections will include the review of samples representing the contractor's derivative classification actions, as applicable.
 - (ii) The contractor will prepare a formal report describing the self-inspection, its findings, and its resolution of issues discovered during the self-inspection. The contractor will retain the formal report for CSA review until after the next CSA security review is completed.
 - (iii) The SMO at the cleared facility will annually certify to the CSA, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification.

Self-Inspection Objectives

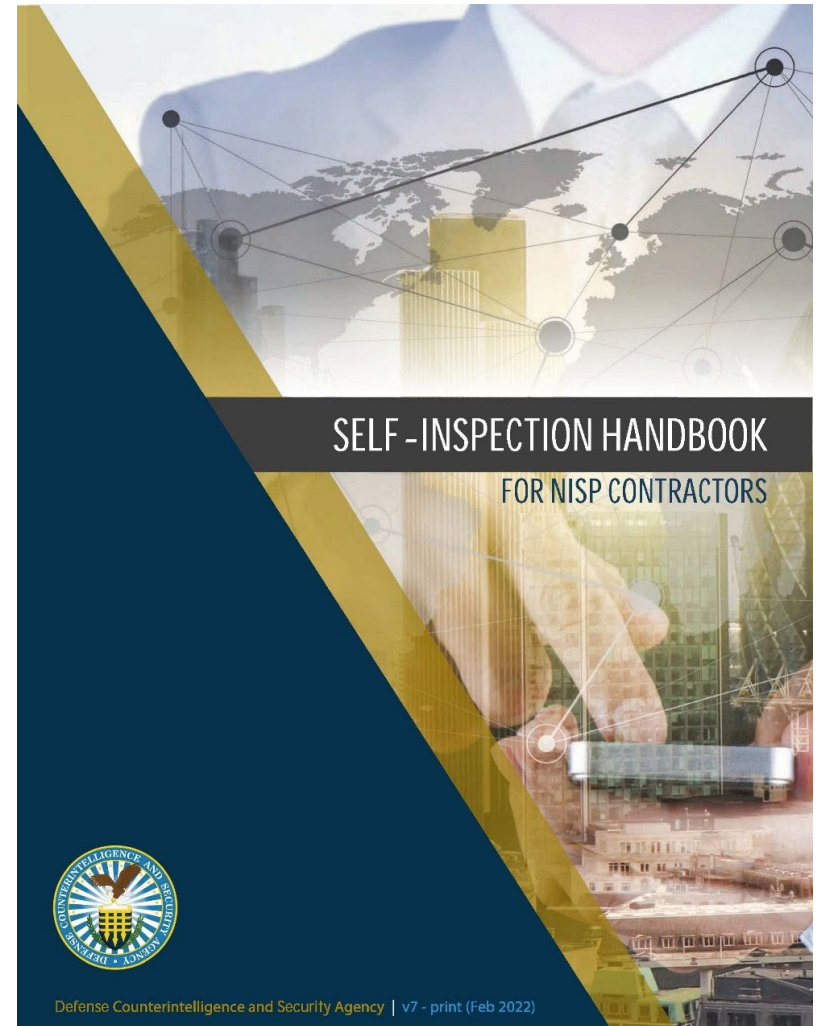


- Evaluate compliance with 32 CFR Part 117 NISPOM Rule
- Review internal processes and identify potential gaps in security controls – **and fix them**
- If applicable, evaluate classified information systems and identify gaps in security controls, **ISSM lead inspection of all classified IS**
- Identify vulnerabilities and administrative findings, then apply, monitor, and track mitigation actions
- Identify best practices and their effective implementation
- Identify security education opportunities
- Brief the results with your SMO and other KMP and receive SMO certification
- Proactively communicate the results with your ISR (and ISSP, if applicable)

DCSA Self-Inspection Handbook (SIH)



- While you are required to conduct a self-inspection, you are not required to use the DCSA Self-Inspection Handbook (SIH)
- Using the tool does help in easily communicating the results with your ISR (and ISSP, if applicable) and discussing mitigation acts and best practices
- Where can I find it? <https://www.dcsa.mil>
 - Click on Mission Centers and select ISD
 - Select Industry Tools
 - Click on FSO Guides
 - Select either the smart form or print version based on your preference





Check all boxes, whether they apply or not – don't risk missing anything

Home
Export All

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	Open Procedures [117.7]
0	0	0	10	Open Reporting Requirements [117.8]
0	0	0	6	Open Entity eligibility determination for access... [117.9]
0	0	0	11	Open (Contractor) eligibility for access to classified... [117.10]
0	0	0	8	Open Foreign Ownership, Control, or Influence (FOCI) [117.11]
0	0	0	10	Open Security training and briefings [117.12]
0	0	0	7	Open Classification [117.13]
0	0	0	14	Open Visits and meetings [117.16]
Safeguarding				
0	0	0	11	Open Marking requirements [117.14]
0	0	0	7	Open General safeguarding [117.15(a)]
0	0	0	1	Open Standards for Security Equipment [117.15(b)]
0	0	0	5	Open Storage [117.15(c)]
0	0	0	14	Open Intrusion Detection System (IDS) [117.15(d)]
0	0	0	11	Open Information Controls [117.15(e)]
0	0	0	13	Open Transmission of classified information [117.15(f)]
0	0	0	3	Open Destruction [117.15(g)]
0	0	0	3	Open Disclosure [117.15(h)]
0	0	0	2	Open Disposition [117.15(i)]
0	0	0	1	Open Retention [117.15(j)]
0	0	0	2	Open Termination of security agreement [117.15(k)]
0	0	0	1	Open Safeguarding CUI [117.15(l)]
0	0	0	7	Open Subcontracting [117.17]
0	0	0	20	Open Information system security [117.18]
0	0	0	31	Open International security requirements [117.19]
0	0	0	8	Open Critical Nuclear Weapon Design Info... [117.20]
0	0	0	6	Open COMSEC [117.21]
Totals				0

10
Self-Inspection Handbook for NISP Contractors

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

117.07-1
Self-Inspection Handbook for NISP Contractors

Self-Inspection Process



- To be most effective, it is suggested that you view your self-inspection as a three-step process:
 - Pre-inspection
 - Inspection
 - Post-inspection
- Pre-Inspection - Preparation for the self-inspection begins with your pre-inspection research and plan:
 - Identify all security checklists that apply to your facility – **choose all**
 - Familiarize yourself with how your company's business is organized (it may have an impact on your company's security procedures)
 - Identify who you will need to interview and what records you may want to review
 - Schedule meetings in advance to allow participants to prepare
 - Prepare a list of questions and topics that need to be covered
 - Know your facility's physical layout (e.g., where the classified material is stored or where it is worked on).
 - Identify the current threats to your company's technologies (contact your assigned counterintelligence special agent, if needed)
 - Have a basic knowledge of your company's classified programs
 - Brief your senior leadership and SMO

Self-Inspection Process



- Inspection

- Conduct inspections with NISPOM SME's and support personnel (FSO/AFSO, IT, ISSM/ISSO, Phys Sec, COMSEC team, CDC personnel, Program employee's and program management)
- Pair less experienced with experienced security professionals; presents an opportunity for development
- Review the self-inspection checklist and quantify processes, procedures and employee actions; not in the 32 CFR, not necessarily a finding
- Talk to employees, explain the self-inspection process, set employee expectations for DCSA audits
- Review Standard Practice Procedures, are you following them? Do employees know where to go to find/access them?
- Have employees demonstrate processes and procedures when possible – **Open ended questions, not yes or no, have them describe/demonstrate**
- Inspect areas, information systems, containers – use checklist style products; take good notes and correct on the spot; involve employees
- **Don't "pencil whip" your inspection, trust but verify and document**
- Meet regularly to discuss deficiencies, corrective actions and need for further review
- Annotate "best practices"

Self-Inspection Process



- 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 (SMO) 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.** IAW 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.
 - **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. **SMO certification required to be uploaded in the National Industrial Security System (NISS), not the actual self inspection.**

Self-Inspection Tips



- Plan accordingly, give your team time to do a thorough self-inspection, **size matters**
- Plan and conduct a kick-off meeting
 - Invite key personnel – set the tone, positive
 - ID 5W's and how, develop a CONOP
 - Set expectations
 - Positive attitudes of security personnel, professional
 - Neat files and records
 - Neat security containers
 - Attention to detail. The small things do count!
 - Facilities clearance and associated data are neatly maintained, easy to get to and well organized
 - Map your approach and ID what you're going to inspect and when
- Self Inspection Products
 - [Findings Tracker](#) spreadsheet or use SIH
 - Build an inspection book with inspection tools
 - [Classified Information System Check Sheet](#)
 - [Classified marking example sheet for documents and media](#)
 - Classified marking guides (all years)
 - [Questions for cleared and uncleared employees](#)
 - [OSA inspection checklists](#)
 - [Container inspection checklists](#)

A	B	C	D	E	F	G	H
Inspector	Date Inspected	Finding	Reference	Actions taken to fix the issue	POC	ECD	Date Corrected
SELF-INSPECTION CHECKLIST							
1		Procedures [117.7]					
2							
3		Reporting Requirements [117.8]					
4							
5		Entity eligibility determination for access... [117.9]					
6							
7		(Contractor) eligibility for access to classified... [117.10]					
8							
9		Foreign Ownership, Control, or Influence (FOCI) [117.11]					
10							
11		Security training and briefings [117.12]					
12							
13		Classification [117.13]					
14							
15		Visits and meetings [117.16]					
16							
17		Marking requirements [117.14]					
18							
19		General safeguarding [117.15(a)]					
20							
21		Standards for Security Equipment [117.15(b)]					
22							
23		Storage [117.15(c)]					
24							
25		Intrusion Detection System (IDS) [117.15(d)]					
26							
27		Information Controls [117.15(e)]					
28							
29		Transmission of classified information [117.15(f)]					
30							
31		Destruction [117.15(g)]					
32							
33		Disclosure [117.15(h)]					
34							
35							

Classified Information System Check Sheet

DATE: _____ BLDG: _____ ROOM: _____ CUBE: _____ ISSO: _____

SYSTEM NAME: _____ SYSTEM NUMBER: _____

IS USER(S): _____

CLASSIFICATION LEVEL: Confidential Secret Top Secret SAP/SAR

CAVEATS: NATO CNWDI RD/FRD CRYPTO FGI

Administrative

1. The system binder has the ATO letter present with an expiration date that has not elapsed.
2. The system binder has the current DD-254(s) for the program(s) being executed.
3. All user account forms have Program Manager endorsement, CPSO clearance verification, and evidence of need-to-know (re)validation within the last year.
4. All privileged user account forms also have a privileged user acknowledgement form signed by the user.
5. The Audit Review Log is present and has a completed date each week indicating weekly audit was conducted.
6. The BIOS password and emergency administrator account password are recorded and stored in a GSA approved safe.
7. The POA&M is present and properly portion marked and properly stored in a GSA container when classified.
8. The continuous monitoring log is present and up to date. Any gaps or incomplete checks have an accompanying MFR or maintenance log entry.


Information System(s)

1. The BIOS is password protected: The BIOS setting menu shows a lock symbol and cannot be unlocked with a blank password.
2. The BIOS boot order is secure: The information system's internal hard drive should be the first item in the boot order. There should be no CD, USB, or PXE boot selected.
3. The BIOS has all wireless disabled: If applicable, any wireless options in the BIOS are disabled or not selected.
4. The information system displays the DCSA approved login banner: Refer to DAAPM Appendix X for correct banner.
5. The screen lock is set and enforces screen lock at 15 minutes: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Machine inactivity limit" to "900" seconds".

Derivative Classification Required Markings

For training purposes only

As of 2021 Marking guide, all final documents or materials, regardless of the media, must have required markings as shown below.

	SECRET//NOFORN (NOTE: This page is Unclassified when removed from contents)	1. OVERALL CLASSIFICATION IN CAPS ONLY
2. Unclassified Title or Subject	(U) Properly Marking a Title Page for Classified Material	*Note: Title or Subject portion marking is <u>now</u> required to be in <i>front</i> .
3. Date of Preparation	June 21, 2013	
4. Name and Address of Generating Facility	 L3HARRIS™ 2400 Palm Bay Road NE Palm Bay FL 32905	
5. Classified By	Classified By: Employee ID #123456 (<i>Unique Identifier</i>)	*Note: Classified By is a new marking requirement.
6. Derived From	Derived From: XYZ Security Classification Guide (SCG), Agency, Dated, June 21, 2003 Downgrade to: if req on date: if req	
7. Declassify On (Date or Event)	Declassify On: 20280621 (yyymmdd) <i>from date document was created</i>	
	SECRET//NOFORN	1. OVERALL CLASSIFICATION SPELLED OUT

- > Additional caveat markings may be required (e.g., NOFORN, NATO, CNWDI, FGI) for special types of material.
- > If derived from multiple sources, include a listing of the source materials in, or attached to, each derivatively classified document/material. The listing may be in the form of a bibliography identifying the creator, title, and date of each source.
- > Each page must have overall classification top and bottom and have **Portion Markings**. All markings indicated above are required for title page. Note that the classification will now proceed the title.
- > Consult your local security representative for any classified marking questions.

8. Example of Portion Markings for Internal Pages –

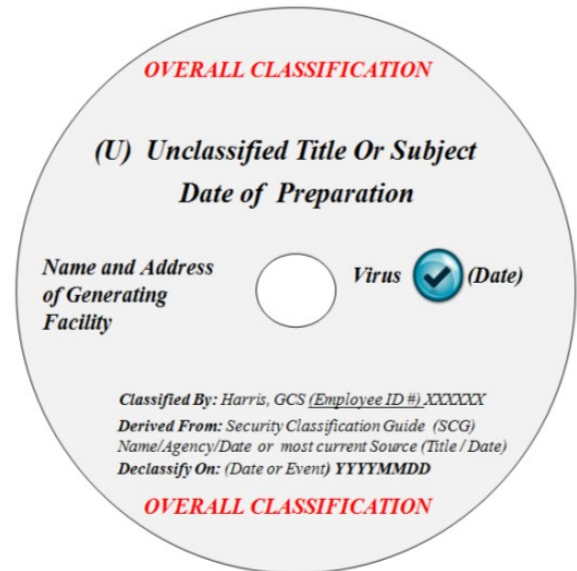
(S//NF) The highest overall classification of the document will be annotated on the top and bottom of every page or you may identify the overall classification of each page independently.

(U) Each section, part, paragraph, graph/picture/photograph or similar portion of material containing classified information shall be portion marked to indicate the highest level of classification.

PROPER MEDIA LABEL

For training purposes only

Title page markings and classification level for media must follow the same requirements as documents



SECURE AREA SELF-INSPECTION CHECK SHEET

DATE: _____ SECURE AREA NUMBER _____ BLDG _____ ROOM _____

PRIMARY CUSTODIAN _____ ISA _____

CLASSIFICATION LEVEL (CIRCLE ONE): SCI SAP Collateral TS Collateral S

OPEN SHELF/BIN STORAGE AUTHORIZED (CIRCLE ONE): YES NO

CAVEATS (CIRCLE ALL THAT APPLY): FGI NATO CNWDI RD FRD COMSEC CRYPTO

EXTERIOR

- The SF702-20 Security Container Check Sheet is present and maintained on the outside of the main door, being properly filled out when opening, closing and conducting all security checks on the secure area
- The prohibited items list, to include portable electronic devices (PEDS), is posted
- The area has been approved by the approving authority and is properly documented (collateral secure areas are approved by DCSA utilizing the DD Form 147)
- Secure areas approved for comingling have proper documentation
- The authorized locking device is working properly, and the combination has been changed as required
- All locking devices and access controls were inventoried (annually)
- The access control device (card reader or cipher lock) is present and operational
- Escorts are properly trained and understand their responsibilities to protect classified material

INTERIOR

- The Area Access List is posted inside the door and is up-to-date
- All custodians and persons having access have been briefed to the highest classification level of the secure area, to include caveats
- A Sec5003 Controlled Area Visitor Log is present and being properly executed and reviewed every quarter
- An Intrusion Detection System is in place, working properly, and has a current Underwriters Laboratory (UL) certification
- Emergency Procedures are posted and identifies the steps required to safeguard classified material in the event of an emergency
- End-of-day security checks are being completed to ensure all classified material is properly secured at the end of each day and the SF701 Security Activity Checklist is being properly executed
- Classified waste has been removed and destroyed IAW 32 CFR Part 117 requirements
- Current DoD Hotline poster is posted in or near the area

Classified Information Systems (IS):

Sec5099 Rev 6/2021

SECURITY CONTAINER SELF-INSPECTION CHECK SHEET

DATE: _____ CONTAINER NUMBER _____ BLDG _____ ROOM _____

PRIMARY CUSTODIAN _____ ISA _____

DRAWERS (CIRCLE ONE): 1 2 3 4 5

CLASSIFICATION LEVEL (CIRCLE ONE) TS S C

CAVEATS (CIRCLE ALL THAT APPLY): FGI NATO CNWDI RD FRD COMSEC CRYPTO

If container has multiple locking drawers, drawer number being inspected _____

EXTERIOR

- The container has no external markings indicating the level of classified material authorized for storage
- The SF 702-20 Security Container Check Sheet is posted at the container and is being properly filled out when opening, closing and conducting all security checks on the container
- The personnel access list is current and is posted on the container
 - *COMSEC controlled containers will have the access list in the interior of the container
- Combination changes are occurring as required
- End-of-day security checks are being completed to ensure all classified material is properly secured at the end of each day
- All custodians have been briefed to the highest classification level of the safe, to include caveats
- The container is outside of an alarmed area, and is being checked by a guard every 4 hours.

INTERIOR

- COMSEC/CCI material is clearly marked
- FGI is properly marked and not comingled with other U.S. classified documents or material
- NATO is properly marked and not comingled with other U.S. classified documents or material and placed in a drawer containing ONLY NATO material
- All working papers are properly marked, dated when created, are within 180 days of creation, marked with their overall classification, and with the annotation WORKING PAPERS
 - *All working papers over 180 days old must be made into a final document or destroyed
- All classified material not currently held under a specific contract (limited retention) are within 1 year of creation date.
 - *All classified documents not under a specific contract are only authorized to be retained for up to 1 year.

Self-Inspection Tips



- Conduct classified material inventories
- Supplemental SIH – add local policies, procedures and instructions to determine if you're following them
- Are you actually doing what you're saying you're doing? Example: **perimeter control checks**: Are you doing them, how often, how do you verify that they are being done, how do you document them?
- Review all DD254's
 - SCG's, OPSEC Plans, PPIPs, TEMPEST requirements, etc.
 - Review subcontracts, ensure GCA approved, no changes in FCL
 - Review NISS for accuracy, update
 - ID what makes your program(s) classified and key personnel (who are the key personnel on the program)
- Consider outside sources to assist with the SI – weary eyes miss things

Questions

