

REMOTE SECURITY REVIEW PREPARATION

FOR NATIONAL ACCESS ELSEWHERE SECURITY
OVERSIGHT CENTER (NAESOC) FACILITIES

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Ronald Young,
Senior Industrial Security Representative
(SISR)





Presentation Overview

Purpose:

To provide Industrial Security Professionals and Senior Management Officials (SMOs) helpful guidance with Remote Security Review (SR) preparation.

Content referenced and derived from:

- DCSA Industrial Security Subject Matter Experts (SMEs)
- 32 CFR Part 117 National Industrial Security Program Operating Manual (NISPOM) – September 2021



Remote Security Review: Facility Criteria

- Active classified work
- Meets NAESOC Criteria
 - No safeguarding
 - Does not fall under formal Foreign Ownership, Control or Influence (FOCI) mitigation
 - Facility had an on-site initial SR
 - Last SR resulted in general conformity



- Not all-inclusive
- Additional risk indicators may warrant an on-site SR



Remote Security Review: High Level Overview



- Industrial Security Representative (ISR) provides notice of Remote SR
- Emailed and included w/in DOD365 Teams Outlook Invite
- Initial request for:
 - Facility profile update
 - Security program documentation
 - Coordination of employee interviews





Notification to Industry

- The invitation is sent to the company's SMO, Facility Security Officer (FSO), and Insider Threat Program Senior Official (ITPSO)
- The facility must provide notice to the ISR of the acceptance of the date and time identified in the notification
- Once Industry accepts the invitation, preparation begins with both DCSA staff and the Industry points of contact (POCs)
- Attached in the notification are resources such as:
 - How to get a National Industrial Security System (NISS) account
 - Submitting a Facility Profile Update Job Aid
 - Messaging in NISS External User Guide
 - SR Employee Interview Scheduler



Security Review: What to Expect



DOD365 Teams is suitable for CUI
Recording is prohibited



Remote SRs will be conducted on DOD365 Teams
You will be able to interact with your ISR on camera



Both the ISR and the facility's security team should
be in a private room with no visible or nearby
distractions, clutter, and with neutral backgrounds



Test audio and video prior to the start time of the
remote SR



Industry Updates: Remote SR Preparation

Prior to the entrance briefing, the FSO is requested to provide company and security program information to DCSA by the listed suspense, to include but not be limited to:

- Facility Profile Update
- Changed Condition Package (if applicable)
- Insider Threat Program Plan
- Standard Practice and Procedures (including SEAD 3 and adverse information reporting procedures)
- ITPSO (and Insider Threat Program personnel) Training Certificate
- FSO (and security staff) Curriculum Completion Certificate
- Self-Inspection Formal Reports since last review (ensure SMO endorsed certification has been completed and uploaded within the NISS self-inspection tab)
- Initial Security Briefing and Annual Security Briefing Training Records
- Special Briefing Records (if applicable)
- Consultant Security Agreements (if applicable)
- Security Violation Reports
- Suspicious Contact Reports and Insider Threat Reports reviewed by the ITPSO
- SR Employee Interview Scheduler



Industry Updates

Changed Condition Package:

A changed condition package must be submitted if there have been any of the following changes to the business :

- Ownership
- Legal Structure/Operating Name
- Key Management Personnel (KMP)
- Principal Address
- FOCI

Facility Profile Update:

Review and complete all sections. Ensure DD254s are attached to active contact submissions.

- If the facility no longer requires an FCL due to no current active classified contracts, the FSO and/or SMO must report this information to DCSA via email and NISS. **32 CFR 117.9 (n)**



Helpful Tips

Employee interviews are essential to DCSA's understanding of the effective implementation of the security program at the facility.

Inform employees of the upcoming security review and begin coordination of their availability.

The employees that DCSA expects to interview are:

- Human Resources (HR)
- Information Technology (IT)
- Subject Matter Experts (SMEs)
- Program Managers (PMs)
- Contract Administrators

The individuals selected and the number of interviews conducted depends on the size and complexity of the facility.



Helpful Tips

Conduct a self-inspection: Contractors shall review their security program on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles. **32 CFR 117.7 (h) (2)**

The self-inspection should include the FSO, ITPSO, SMO, and employee interviews for effectiveness.

Ensure all individuals with insider threat responsibilities have completed insider threat training: Completion of prescribed training is essential in ensuring insider threat program personnel possess the required knowledge to identify and report insider threat indicators and to help effectively manage the insider threat program. The ITPSO shall ensure that this training is completed. **32 CFR 117.12 (g)**

Ensure all security officers have completed FSO training: Contractors will ensure the FSO and others performing security duties complete training considered appropriate by the CSA. **32 CFR 117.12 (d)**



Resources

- [Security Review Process Slicksheet](#)
- [Security Rating Process Slicksheet](#)
- [32 CFR Part 117](#)
- [FSO Toolkit](#)
- [Self-Inspection Handbook](#)
- [NAESOC Webpage](#)
- [NCAISS/NISS](#)





Contact Us

- NAESOC Knowledge Center: 1 (878) 274-1800
and/or email:

Include Facility Name & CAGE Code on the SUBJECT LINE:

- For *General Questions/Feedback*: dcsa.naesoc.generalmailbox@mail.mil
- To report *Changed Conditions*: Create a changed condition package in NISS. If you have an upcoming changed condition or have questions regarding submitting a changed condition package, email the General Mailbox above.
- To report *Security Violations*: NISS Messenger labeled "Message My ISR."