# Personnel & Facility Security Trends in 2024

## DCSA and MPO Policies, Systems, Updates

Guest Speakers

Megan Couch, CSSO/FSO, JASINT Consulting & Technologies, LLC

Kathy Butler, CSSO/FSO, Nexxis Solutions, Inc

# TOPICS

- NISP & SMO Responsibilities
- Facilities Clearance
- SEAD 3 Reporting Requirements
- Training
- Briefings – SF312, NATO
- Records Retention
- DISS & NBIS
- Continuous Vetting / Evaluation (CV/CE)
- MPO – Personnel Clearances
- MPO – Portal

# NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

- Understanding and general overview the NISP as it applies to your company
- Expectations for senior leaders in the company supporting it
  - ie: training (through STEPP), compliance, inspections, etc.
- Senior Management Official (SMO) briefing
- SMO understanding of his/her roles/NISP responsibilities

# NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

- An application within the DCSA's NCAISS portal
- System of record for Facility Clearances (FCL)
- Requires users have either a DoD Common Access Card (CAC) or an External Certification Authority (ECA) PKI certificate

NISS is also used when a Prime is submitting new DD254's or DD254's for revision. It allows you to setup ongoing request updates for other company's facility clearances so you are notified if anything changes under their cage code.

# FACILITIES CLEARANCES

The facilities clearance (FCL) is a determination made by the Government that a contractor is eligible for access to classified information. A contractor must have an FCL commensurate with the highest level of classified access (Secret or Top Secret) required for contract performance.

**The process to be considered for a security clearance:**

- Request Cage Code in SAMS.
- Identify a prime sponsor that is willing to request a government approval for an FCL. This usually requires that the company needing sponsorship supplies some sort of skill or device that will be beneficial to the contract mission. *This is where business development is involved.*
- Once prime has submitted sponsorship request to DCSA through NISS, company will need to create NISS account, and fill out all necessary paperwork with DCSA directly. THIS IS TIME SENSITIVE.
- DCSA makes determination of adjudication for granting the FCL or not.

# SENIOR MANAGEMENT OFFICIAL (SMO) BRIEFING & ANNUAL CERTIFICATE

- Annual SMO briefing and certificate required to be submitted to DCSA

Pursuant to the provisions of 32 CFR Part 117, the National Industrial Security Program Operating Manual (the "NISPOM"), and the Department of Defense (DoD) Security Agreement; under which I have been designated as the Senior Management Official (SMO), the following assurances are provided:

1. I am a U.S. citizen currently residing within the continental United States, capable of assuming full responsibility for the company's policy and strategy, and I have ultimate authority of the business operations of Nexxis Solutions, Inc. (Nexxis) and the authority to direct actions necessary for the safeguarding of classified information within the facility, specifically Nexxis' cleared facility, and any current or future cleared subsidiaries, commensurate with the size and complexity of security operations.

1. I have and will maintain a personal security clearance to the same level as Nexxis' Facility Clearance Level (FCL).

1. In accordance with NISPOM section (§) 117.7(b)(2), I will:
   (i) Ensure Nexxis implements and maintains a system of security controls in accordance with NISPOM requirements.
   (ii) Appoint, in writing, Nexxis' Security Officials per §117.7(b), the Facility Security Officer (FSO) and Insider Threat Program Senior Official (ITPSO).
   (iii) Remain fully informed of the facility's classified operations.
   (iv) Make business decisions based on classified threat reporting and my thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss or compromise of classified information.
   (v) Retain accountability for the company's management and operations without delegating that accountability to a subordinate manager.

1. I fully understand my role and responsibilities as Senior Management Official, and I accept those responsibilities.

- Signed: SMO Name & Date

# SMO RESPONSIBILITIES

- 32 CFR Part 117 is a federal rule that provides the National Industrial Security Program Operating Manual (NISPOM) and **required contractors to comply with its security requirements by August 24, 2021**
- 32CFR has the SMO responsibilities in a bullet format (32CFR Part 117.7.b.2):
- (2) SMO. The SMO will:
- (i) Ensure the contractor maintains a system of security controls in accordance with the requirements of this rule.
- (ii) Appoint a contractor employee or employees, in writing, as the FSO and appoint the same employee or a different employee as the ITPSO. The SMO may appoint a single employee for both roles or may appoint one employee as the FSO and a different employee as the ITPSO.
- (iii) Remain fully informed of the facility's classified operations.
- (iv) Make 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.
- (v) Retain accountability for the management and operations of the facility without delegating that accountability to a subordinate manager.

# SEAD 3

- SECURITY EXECUTIVE AGENT DIRECTIVE (SEAD) 3 Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position was established to standardize reporting across the federal government and in a timelier manner.
- Covered individuals: Individuals (to include contractors, subcontractors, licensees, certificate holders, grantees, experts, and consultants) who:
  - Perform work for or on behalf of the executive branch who have been granted access to classified information or who hold a sensitive position,
  - Perform work for or on behalf of a state, local, tribal, or **private sector entity, who have been granted access to classified information**; or
  - Serve in the legislative or judicial branches and have been granted access to classified information

- Most of the requirements are not new but one change is reporting unofficial foreign travel in the DISS system of record

Access the entire policy briefing here: SEAD-3-awareness-briefing.pdf (dni.gov)

# TRAINING

| Training & Authority | Why | When | Who | Length |
|---|---|---|---|---|
| **Security – Defense Counterintelligence & Security Agency (DCSA)/ North Atlantic Treaty Org. (NATO)** | Classified Protection | Annually in December | Anyone granted access by their customer | < 1/2 hour |
| **Security – ITAR (Dept. of State)** Note: ITAR Training may be billable to the contract | Export Control | As needed per program | Any Employees & 1099s who are on a program that exports | ~ 1/2 - 1 hour |
| **Security – Annual Refresher with SPP Review (DCSA)** | Security regulations | Initially then Annually in January | All Employees & 1099s | ~ 1/2 - 1 hour |
| **Security – SEAD 3 Reporting (DCSA)** | Reporting requirements | Annually in January | All Employees & 1099s | ~ 1/2 hour |
| **Security – PII & Civil Liberties (DCSA)** | Protecting PII data | Annually in January | All Employees & 1099s | < 1/2 hour |
| **Security – CUI (DCSA)** | Protecting CUI data | Annually in January | Once this is incorporated into our contracts then it will apply to All Employees & 1099s | ~ 1/2 - 1 hour |
| **Security – Derivative Classification (DCSA)** | Appropriately classifying material | Annually in January | All Employees & 1099s | ~ 1/2 hour |
| **Security – Insider Threat Program (DCSA)** | Identifying and reporting insider threats | Initially then Annually in September | All Employees & 1099s | ~ 1/2 - 1 hour |
| **Security – Insider Threat Program Working Group (ITPWG) (DCSA)** | Identifying and reporting insider threats | Initially then Annually in September | All Principals, Directors, PMs, and Department Heads | ~ 1 - 2 hours |
| **Security – Cyber Awareness Challenge (DCSA)** | Identify & mitigate threats & vulnerabilities to DOD Information Systems | Annually in January | All Employees & 1099s | ~ 1/2 - 1 hour |
| **HR – Ethics & Harassment (State and Local Laws)** | Discrimination and anti retaliation | Annually in January | All Employees & 1099s | < 1/2 hour |
| **Accounting – Timekeeping Policy Acknowledgement (DCAA)** | Submitting timekeeping records | Annually in January | All Employees & 1099s | < 1/4 hour |
| **Security – overall awareness training campaign (DCSA)** | Continuous security awareness | Ongoing | All Employees & 1099s | < 1/4 hour each |

# RECORDS RETENTION

- Your Government Cognizant Authority (GCA) [DCSA and NSA and other customers] requires retention of certain records with varying time frames for both facility and employee records
- While there are specific retention period requirements, caveat that with AND until your next DCSA/NSA/GCA inspections
- We have compiled the list from multiple sources across NSA and DoD.
  - A separate handout is here, but it is also available electronically along with these slides

# DISS & NBIS

- Defense Information System for Security
  - Defense Information System for Security (DISS) (dcsa.mil)
  - DISS is still the enterprise-wide system of record for all personnel clearance actions EXCEPT SF-86s
    - Historical SF-86 archival copies
      - *Copied from DISS:* Due to Industry's need to obtain subjects' historical SF86 Archival Copies, DISS will be reopening the Investigation Request Link to initiate investigations through e-QIP. This function is part of DISS Release 13.22.0 which is scheduled to be released January 25, 2024. This will provide subjects with the ability to log into e-QIP and download historical archival copies. DISS will automatically cancel these requests in both DISS and e-QIP after 7 days. It is important to note that requests will only be initiated to pull historical copies until the function moves over to NBIS. New requests for background investigations or Continuous Vetting updates/enrollments will continue to be completed via NBIS.
- National Background investigation Services
  - National Background Investigation Services Agency Portal (nbis.mil)
  - Sign up for NBIS – https://dcsa.servicenowservices.com/nbis
    - Complete the PSSAR form
    - Provide certificates of training with last 12 months for PII & Cyber Challenge
    - Repeat these steps for your backup/alternate user
  - Basic maneuverability in the system for subject management
    - Create an account on Security Training, Education, and Professionalization Portal
      - STEPP: Frequently Asked Questions (usalearning.gov)
        - Lots of webinars for industry
- SF-86/eAPP processing
- System is still evolving

# CONTINUOUS EVALUATION / VETTING (CE/CV)

Responsible for ensuring a Trusted Workforce 2.0

- The CV process may include the following:
- Tier 5 Reinvestigations through DCSA for collateral clearance
  - (Reinvestigation packages due every 5 years for both Secret and Top Secret)
    - Example, DISS says: Last investigation date 25-Dec-2020
    - CE Date 17-Mar-2021
    - Submit new investigation 90-before 17-Mar-2026
- Enrollment in CV/CE is a series of automated datasets that will alert on things such as clearance eligibility, terrorism, foreign travel, criminal activity, suspicious financial activity, credit and commercial checks.
- Can lead to an investigation
- Enrollment in RAPBACK Program (FBI "Record of Arrest and Prosecution Background" program)
- Aperiodic Polygraph Examinations
- Annual Vetting Appraisal (AVA) at NSA
  - Annual assessment containing 17 questions that is sent out during month of birth for completion
  - Still in testing phase
- Insider Threat Programs, activity monitoring, investigations and self reporting

- MPO - Continuous Vetting, A5421 (formerly Reinvestigations)
  - Provide decisions regarding continued eligibility for NSA SCI access

# DOD CLEARANCES

- Confidential
- Public Trust
- Secret
- Top Secret
- Top Secret/SCI
- TS/SCI with Polygraph (CI or FS)

*interim clearances are permitted by some programs

# MPO PERSONNEL CLEARANCES

- Clearance Package Processing Timeframes (add 4+ weeks for Indoc scheduling)
  - Single-Track (S/T) – 18-24 months
    - Nominee had TS but has never had SCI access OR has been out of SCI access for more than 2 years; SSBI is within the last 7 years; Requires a PG
  - Dual-Track (D/T) – 14-18 months
    - Nominee has never had TS clearance or access to SCI OR Nominee has been debriefed from TS clearance or SCI access for more than 24 months and the BI is more than 7 years old - Requires BI & PG
  - Conditional Certification of Access (CCA) – 6+ months (CCA's are being opened that were submitted in August and was told there are 700+ packages in the queue.
    - Nominee is currently in SCI access with another government agency or military service OR nominee has been debriefed from SCI access with another government agency or military service within the past 2 years
      - Must have current CI Polygraph and requires FS Poly prior to clearance approval
      - CCA with issues: Almost always converted to a ST (18-24 months)
  - Reinstatement (Rein) – averaging 2 weeks processing time
    - Nominee is currently in SCI access with NSA OR Nominee has been debriefed from NSA SCI access for less than 2 years OR if Nominee has been approved for NSA SCI access less than 12 months and has not been indoctrinated
      - Must have Full Scope Polygraph
      - Reinstatement with issues: Case by case; 3 months or longer

- Polygraphs & Special Accesses
  - Polygraph processing is still very backlogged
    - NSYS or other special accesses may be at risk of being denied future access if you are changing programs or companies AND your polygraph date falls out of scope for the new program (ie: 5 or 7 years). A5 security will not budge on the polygraph timeline requirements when moving contracts

# MARYLAND PROCUREMENT OFFICE
# MPO WEBSITE

- eSponsorship website was implemented in May 2022, updated in January 2024
  - Contracts and Accounting utilize for processing contracts and invoices, labor, grants, GFP, CDR, CAP, Self-Assessments
  - All Security packages are now submitted electronically
    - DD254s
    - Sponsorship Letter / Clearance Packages
    - SCIF Workflow Accreditation Records Management (SWARM)

- To gain access to the MPO website, a DoD CAC or a ECA PKI Certificate is required

- Send email to dialogue@ec.ncsc.mil with ECA Certificate or CAC certificate as a .txt file requesting access.

- Contact EC help desk - 410-854-5445 - https://mpo.ec.ncsc.mil

# Questions?

Megan Couch, CSSO/FSO
JASINT Consulting & Technologies, LLC
mcouch@jasint.com
410-969-5573 ext 707

Kathy Butler, CSSO/FSO
Nexxis Solutions, Inc
kabutler@nexxissolutions.com
443-306-9645