STANDARD PRACTICE AND PROCEDURES

Table of Contents

1. **PURPOSE**. The Standard Practice and Procedures (SPP) provides the structure for compliance with Industrial Security Letter (ISL) 2021-02 for implementation of the reporting requirements set forth in Security Executive Agent Directive 3 (SEAD-3) and Adverse Information Reporting as directed by 32 CFR Part 117 (NISPOM) 117.8(c)(1). Effective compliance with the listed guidances is necessary for effective training, tracking, and reporting of relevant security information for personnel approved for access to classified information.

2. **COVERED INDIVIDUALS**. The SPP applies to all Cleared Employees as defined in 32 CFR Part 117.3(b) and consultants meeting the requirements set forth in 32 CFR Part 117.10(m). Reporting requirements are established based on the highest level of eligibility regardless of current access (e.g., employee with Top Secret eligibility and Secret access will follow reporting requirements for Top Secret).

3. **RESPONSIBILITY**. The Facility Security Officer (FSO) has been appointed by the organization's Senior Management Official and has been granted authority within the organization to supervise and direct security measures necessary for implementing the SPP and any related security requirements to ensure the protection of classified information. As such, the FSO will be responsible for selecting, creating, or directing the creation of, all applicable training materials required to meet the requirements of the SPP, as well as providing such training as required, and will be responsible for oversight of all report tracking as required. The FSO may designate another individual to assist with the requirements of the SPP. Any designee will complete commensurate training necessary to properly manage any assigned actions or activities.

4. **TRAINING**.

4.1. Reporting Requirement Training. Training covering adverse information reporting will be provided to all personnel defined in the Scope upon any of the following events:

- Submission of an Investigation Request for classified access for an individual that previously did not hold eligibility for classified access.
- Start of employment for an individual that holds eligibility for classified access at the time of hiring and if that individual will not be receiving Initial Security Training.
- Completion of a consultant agreement when the consultant holds eligibility for classified access at the time the consultant agreement goes into effect and if that individual will not be receiving Initial Security Training.

Reporting Requirement Training will, at a minimum, identify adverse and other information reporting requirements set forth in SEAD-3, ISL 2021-02, unofficial foreign travel reporting

processes, provide a definition of Adverse Information as set forth in 32 CFR Part 117.3(b), and identify reporting procedures for such information relating to individual and other covered individuals.

4.2. Initial Training. Prior to being granted Classified Access, personnel will receive Initial Training which includes the information contained within the Reporting Requirement Training, and will additionally receive training which meets the requirements of 32 CFR Part 117.12 to provide personnel with an understanding of their individual responsibility for safeguarding classified information, threat awareness, counterintelligence awareness, an overview of the information security classification system, the company's graduated scale of administrative and disciplinary actions, and any additional reporting obligations and processes as set forth in 32 CFR Part 117, SEAD-3, and any relevant ISL's. Initial Training will also include security procedures and duties specific to the individual's position.

Insider Threat Awareness that complies with 32 CFR 117.12(g) will also be provided with Initial Training.

Initial Training may be provided in lieu of Reporting Requirement Training.

4.3. Annual Refresher Training. All personnel that receive Initial Training will be provided with additional training, at least annually, which meets the requirements of 32 CFR Part 117.12(k) and reinforces the information provided during the initial security briefing, with specific focus on reporting requirements and procedures.

4.4. Additional Training. The FSO will identify when additional training is required outside the Annual Refresher Training cycle for the purpose of informing cleared personnel regarding changes in security regulations or policies and will address issues or concerns identified during internal security reviews.

5. **ADVERSE INFORMATION REPORTING**. Reports of all Adverse Information, events, or actions will be submitted to the FSO, or their designee. Submission of reports may be made in-person, by phone, or via e-mail. Reports containing classified information or Controlled Unclassified Information may only be submitted through channels approved for such information. Personnel should contact the FSO if they require assistance with identifying an approved transmission method for such information.

The FSO, or their designee, will be responsible for investigating reports of adverse information to determine validity. Only verified adverse information will be approved for submission and no report will contain information based on rumor or innuendo. Any investigation of verified adverse information will include the collection of Required Data Elements for Reporting, as set forth in

SEAD-3 Appendix A, or any additional data required for submission in the DoD-designated system of record. All reports will be maintained in a manner which precludes their access by unauthorized personnel.

Verified reports of adverse information, not previously submitted in an SF-86 or in the Defense Information System for Security (DISS), will be reported by the FSO, or designee, through the DoD-designated personnel security system of record. DISS is the current DoD system of record for personnel security management as set forth in 32 CFR Part 117.5(d).

The process for managing the information reporting is provided via flowchart in Attachment 1.

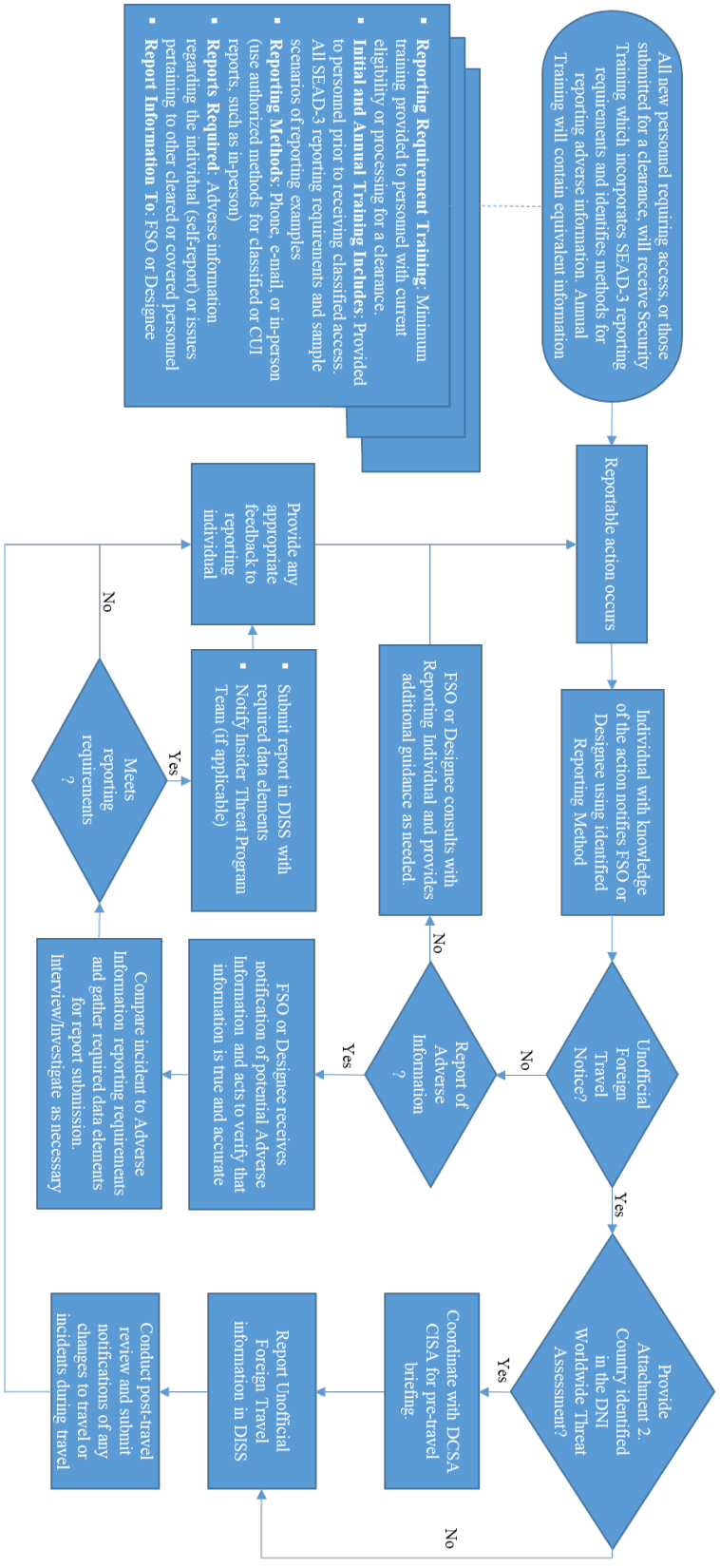
6. **UNOFFICIAL FOREIGN TRAVEL REPORTING**. All covered individuals will report Unofficial Foreign Travel to the FSO, or designee, at least 5 business days prior to travel (unless precluded from this requirement based on ISL 2021-02 Table 4 exceptions). The FSO, or designee, will provide Attachment 2 to the covered individual for the purpose of collecting reportable data elements and to advise the individual of travel resources set forth in ISL 2021-02 Table 4.

The FSO, or designee, will review reported information in Attachment 2 to determine if coordination with a Defense Counterintelligence Security Agency Counterintelligence Special Agent.

FSO, or designee, will contact the covered individual post-travel to identify if any reportable irregularities occurred during the trip.

7. **ADDITIONAL INCIDENTS OR ACTIONS**. The FSO will be responsible for identifying any additional reporting requirements or activities which may not be outlined within the SPP, but which may potentially impact any classified activities or negatively affect cleared personnel.

ATTACHMENT 1: **INFORMATION REPORTING FLOWCHART**



ATTACHMENT 2: **FOREIGN TRAVEL REPORTING AND ADVISEMENT**

Please complete Part 1 and review Part 2, then return the form to the security office. Be aware of additional reporting requirements for items in Part 3 upon return. Reporting and information on this form complies with the requirements set forth in SEAD-3 and ISL 2021-02 and are required for all cleared personnel engaging in unofficial foreign travel.

Part 1: Prior to travel. Please fill this section in now.

Dates of Travel:	
Complete Itinerary:	
Mode of Transportation and Identity of Carrier:	
Passport Data:	
Name and association (business, friend, relative, etc.) of foreign national traveling companions (if applicable):	
Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.):	
Name, address, telephone number, and relations of emergency point of contact:	

Part 2: Prior to travel. Please review and be aware of the following information.

- ✓ Review the NCSC "Safe Travels" resource at: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf

- ✓ Review the Department of State Travel Advisories to determine if any of your travel (including layovers or transfers) will be in a country with an existing advisory. Review any such advisories prior to travel and contact the security office if you have any questions: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

Part 3: Upon the completion of your travel, please notify security if any of the following occurs:

Unplanned contact with foreign governments, companies, or citizens during travel and reason for contact.
Unusual or suspicious occurrences, including those of possible security or counterintelligence significance.
Any foreign legal or customs incidents encountered
Any changes that occurred regarding your submitted itinerary (e.g., unplanned layovers, diverted flights, etc.)