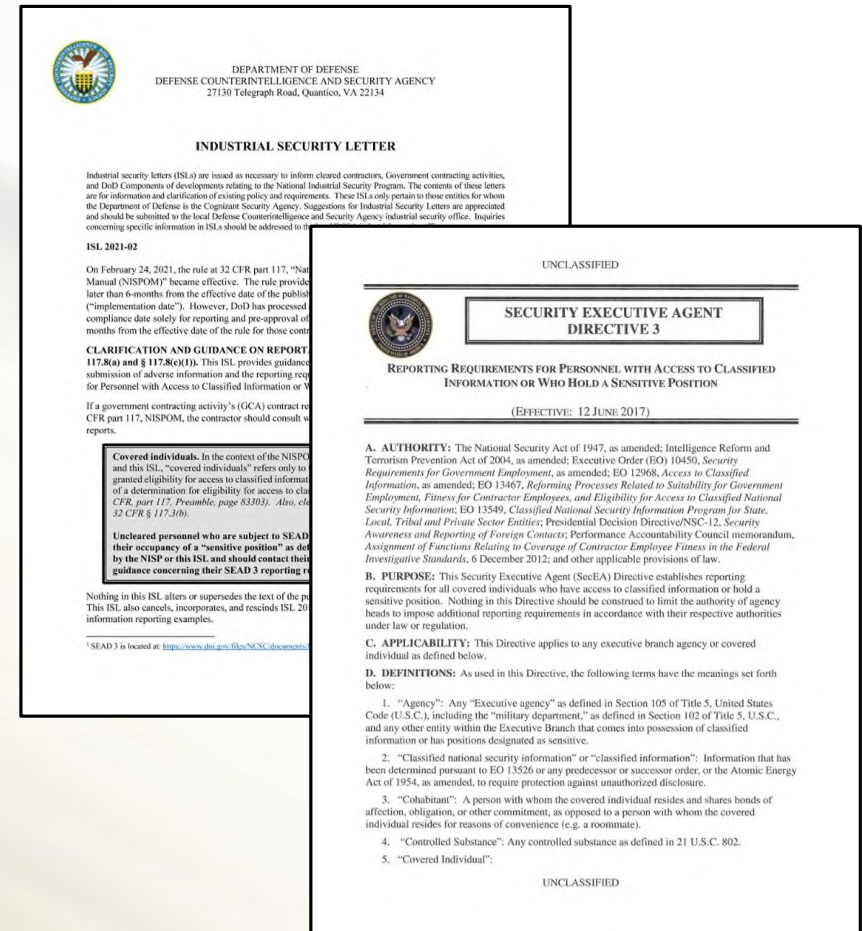


SEAD-3 Reporting Requirements & Standard Practice Procedures

**Justice Exum
Will McEllen**





Adverse Information

ADVERSE INFORMATION, as defined by 32 CFR 117.3(b), means any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes an insider threat.

32 CFR 117.8(c) provides the requirement for Contractors to report adverse information coming to their attention concerning any of their employees *determined to be eligible for access to classified information*, in accordance with this rule, SEAD-3, and Cognizant Security Agency provided guidance. Note that reports must not be based on rumor or innuendo.



Adverse Information

Cleared personnel are required to report adverse information about themselves as well as other cleared individuals that they come into contact with.

Reports may be made through multiple channels (e.g., e-mail, phone, or in-person) as identified by the company's security plan or guidance. It is also important to note that reports which contain Classified or Controlled Unclassified Information (CUI) can only be submitted through channels approved for the transmission of such information.

32 CFR 117.5(d) – Identifies DISS as the system within DoD for submitting adverse information



13 Adjudicative Guidelines

The 13 Adjudicative Guidelines are used by Adjudicators to make determinations for eligibility to access classified. You can reference these guidelines, along with concerns and mitigations, in SEAD-4.

The additional reporting requirements in SEAD-3 expand on certain requirements for the 13 Adjudicative Guidelines and provide more direct guidance for select situations.

The goal is for personnel to be aware of these new requirements and report any information regarding their own, or other's, behavior that is not consistent with, or that violates, the 13 adjudicative guidelines.

CDSE Training: Personnel Security Shorts

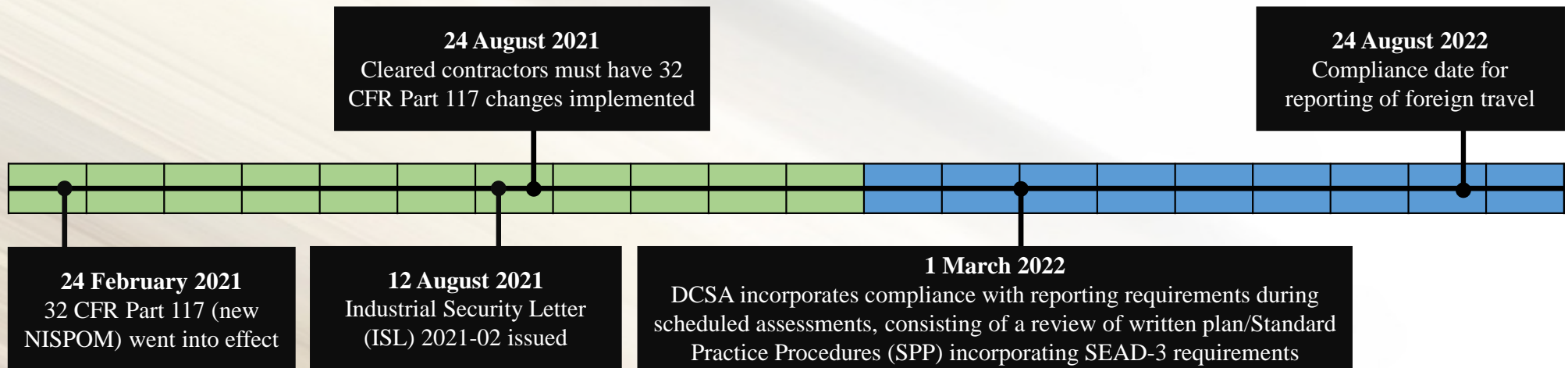
<https://www.cdse.edu/Training/Security-Shorts/Personnel-Security-Shorts/>

- Adverse Information Reporting
- Continuous Evaluation Awareness
- Personnel Vetting At A Glance
- Reporting Requirements At A Glance
- Each of the 13 Adjudicative Guidelines
- The Federal Investigative Standards



- A: Allegiance to the United States
- B: Foreign Influence
- C: Foreign Preference
- D: Sexual Behavior
- E: Personal Conduct
- F: Financial Considerations
- G: Alcohol Consumption
- H: Drug Involvement and Substance Abuse
- I: Psychological Conditions
- J: Criminal Conduct
- K: Handling Protected Information
- L: Outside Activities
- M: Use of Information Technology

SEAD-3 Notable Dates and Compliance



DCSA requires that the contractor's written plan/SPP will, at a minimum, establish the necessary processes and procedures to inform their cleared contractor personnel on reporting requirements related to SEAD-3 and the requirements for adverse information reporting as directed by 32 CFR Part 117.8(c)(1). It must also include processes and procedures that address:

- ✓ How the contractor receives, processes, and manages the required reports for SEAD-3.
- ✓ How these processes and procedures are to be implemented within the cleared contractor facility.
- ✓ How a covered individual will alert the cleared contractor (FSO or assigned designee) of the reportable actions concerning other covered individuals.

SEAD-3/ISL 2021-02 Reporting Requirements Based on Level of Eligibility



**CONFIDENTIAL
SECRET
'L' ACCESS**



**TOP SECRET
'Q' ACCESS**

Note that reporting is based on *ELIGIBILITY* and not just *ACCESS* and includes individuals processing for a clearance.

Information for Reports (SEAD-3 Appendix A and ISL 2021-02 Tables)

SEAD-3 Appendix A contains listings of data elements which are requested when submitting reports.

APPENDIX A REQUIRED DATA ELEMENTS FOR REPORTING

When self-reporting or reporting about others is necessary, the following information must be provided in the report, as available and applicable.

1. Foreign travel:
 - a. Complete itinerary.
 - b. Dates of travel.
 - c. Mode of transportation and identity of carriers.
 - d. Passport data.
 - e. Names and association (business, friend, relative, etc.) of foreign national traveling companions.
 - f. Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.).

ACTIVITY CATEGORIES	CONTRACTOR GUIDANCE & CLARIFICATION FOR REPORTING BY <u>ALL</u> COVERED INDIVIDUALS	TYPES OF REPORTING REQUIRED BY CLEARED CONTRACTOR (FSO OR ASSIGNED DESIGNEE) IN DISS OR SUCCESSOR SYSTEM	REQUIRED DATA ELEMENTS FOR SUBMITTED REPORTS
Personal Finance & Business Interests	<p>Cryptocurrency. Ownership of foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges.</p> <p>No reporting is required if the covered individual holds cryptocurrency, but is NOT aware that any such holdings are backed, hosted, or managed by a foreign state, or that a cryptocurrency wallet is hosted by a foreign exchange.</p> <p>No reporting is required if the covered individuals investments in cryptocurrency are held in a widely diversified fund (e.g. index funds), unless the investment instrument is entirely composed of holdings in cryptocurrency that is backed, hosted, or managed by a foreign state.</p>	Incident Customer Service Report entered	<ul style="list-style-type: none">• Name of cryptocurrency• Exchange host country• Dollar value of the asset

ISL 2021-02 contains Tables which help identify what type of report to submit and provides additional data elements for some reports.

Reporting Aid



SEAD 3 INDUSTRY REPORTING DESKTOP AID

REPORTABLE ACTIVITY	SECRET AND "L"	TOP SECRET AND "Q"	REFERENCE SEAD 3	REFERENCE ISL TABLE
Foreign Contacts (Official)	YES	YES	D.8; F.2.a; Appendix A.2. and A.3.	2
Foreign Contacts (Unofficial)	YES	YES	D.8; F.2.b.2.; Appendix A.2.	2
Behavior and Conduct (Reportable By Other Covered Individuals)	YES	YES	F.3.; Appendix A As Applicable	2
Behavior and Conduct (Attempted Elicitation, Exploitation, Blackmail, Coercion or Enticement)	YES	YES	G.1.a.; H.1.d.; Appendix A.13.	2
Foreign Affiliation; application for or receipt of foreign citizenship	YES	YES	G.1.a.; H.1.d.; Appendix A.7.	2
Media Contact	YES	YES	G.2.d.; H.2.b.; Appendix A.14.	2
Criminal Activity	YES	YES	G.2.c.; H.2.c.; Appendix A.15.	2
Treatment and Counseling	YES	YES	G.2.3.; H.2.h.; Appendix A.19.	2
Personal Finance and Business Interests	YES	YES	G.2.d; H.2.d.; Appendix A.16.	2
Foreign Affiliation; voting in a foreign election	NO	YES	H.1.f.; Appendix A.11.	3
Personnel Finance and Business Anomalies; financial anomalies	NO	YES	H.2.d.; Appendix A.16.	3
Personnel Finance and Business Anomalies; direct involvement in financial business	NO	YES	H.1.a.; Appendix A.4.	3
Personnel Finance and Business Anomalies; foreign bank accounts	NO	YES	H.1.b.; Appendix A.5.	3
Personnel Finance and Business Anomalies; ownership of foreign properties	NO	YES	H.1.c.; Appendix A.6.	3
Living Status/Arrangements; cohabitation	NO	YES	H.1.c.; Appendix A.6.	3
Living Status/Arrangements; marriage	NO	YES	H.2.g.; Appendix A.18.	3
Living Status/Arrangements; adoption of non-U.S. citizen children	NO	YES	H.1.g.; Appendix A.12.	3
Living Status/Arrangements; foreign national roommates	NO	YES	D8; H.2.3.; Appendix A.3.	3

Reporting Aid



SEAD 3 INDUSTRY REPORTING DESKTOP AID

REPORTABLE ACTIVITY	SECRET AND "L"	TOP SECRET AND "Q"	REFERENCE SEAD 3	REFERENCE ISL TABLE
Foreign Travel (Unofficial) ^{1,2}	YES See Footnotes	YES See Footnotes	F.1.b.; Appendix A.1, items e, f, h, and as needed g, i, and j	4
Foreign Travel (Unofficial), deviations from submitted travel itinerary ^{1,2}	YES See Footnotes	YES See Footnotes	F.1.b.1.	4
Foreign Travel (Unofficial), unplanned trips to Canada or Mexico ^{1,2}	YES See Footnotes	YES See Footnotes	F.1.b.(b)	4
Foreign Travel (Unofficial), emergency circumstances ^{1,2}	YES See Footnotes	YES See Footnotes	F.1.b.1.(d)	4

¹ DoD has amended 32 CFR Part 117, the NISPOM Rule to extend the compliance date solely for foreign travel reporting until no later than 18 months from the effective date of the rule for those contractors under DoD security cognizance. The reporting of the foreign travel component of SEAD 3 must begin no later than August 24, 2022.

² Contractors should consult with their government customers for reporting of foreign travel for those personnel who have SCI or SAP access and/or additional contractual reporting requirements.

References

[Security Executive Agent Directive 3, "Reporting Requirements for Personnel Who Access Classified Information or Who are in a Sensitive Position"](#)

[ISL 2021-02, Security Executive Agent Directive 3, "Clarification and Guidance on Reportable Activities"](#)

Psychological and Emotional Health (ISL 2021-02, Table 1)
Required for: All Covered Individuals

Consistent with Section 21 of the Questionnaire for National Security Positions (SF-86), covered individuals should report **psychological and emotional health conditions** that involves the following situations:

- A court or administrative agency issued order declaring the individual to be mentally incompetent.
- A court or administrative agency ordering the individual to consult with a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.).
- Hospitalization of the individual for a mental health condition.
- Diagnosis of the individual by a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.) of psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial personality disorder.
- Occasions within the last seven years where the individual did not consult with a medical professional before altering, discontinuing, or failing to start a prescribed course of treatment for any of the above diagnoses. Details of any current treatment for the above diagnoses must be reported.
- Any mental health or other health condition that the employee feels substantially and adversely affects their judgment, reliability, or trustworthiness regardless of current symptoms.

Cryptocurrency (ISL 2021-02, Table 1)

Required for: All Covered Individuals

Ownership of foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges.

No reporting is required if the covered individual holds cryptocurrency but is NOT aware that any such holdings are backed, hosted, or managed by a foreign state, or that a cryptocurrency wallet is hosted by a foreign exchange.

No reporting is required if the covered individual's investments in cryptocurrency are held in a widely diversified fund (e.g., index funds), unless the investment instrument is entirely composed of holdings in cryptocurrency that is backed, hosted, or managed by a foreign state.

As an example, here are some exchanges whose use would require reporting:

BitMEX (Hong Kong)	ZB.COM (Samoa)
HitBTC (Hong Kong)	Binanace (Multiple Locations Asia)
Bibox (China)	Upbit (South Korea)
Bithumb (South Korea)	Bit-Z (Singapore)



If a report is required, submit an Incident Report in DISS and provide the following data elements:

- Name of cryptocurrency
- Exchange host country
- Dollar value of the asset

Unofficial Foreign Travel (SEAD-3, F.1.b)

Required for: All Covered Individuals

Unofficial Foreign Travel is defined as all travel other than that defined by “official foreign travel,” and includes any foreign travel conducted before, during, or after official foreign travel, and that does not meet the criteria of “official foreign travel”.

Official Foreign Travel is defined as foreign travel by covered individuals that is in direct support of an established U.S. Government contract with the ultimate customer being the U.S. Government, whether as a prime contractor or a sub-contractor.

Not Reportable: Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and does not need to be reported.



Unofficial Foreign Travel (SEAD-3, F.1.b)

Required for: All Covered Individuals

SEAD-3 requires pre-approval prior to unofficial foreign travel. DoD considers unofficial foreign travel by a covered individual under DoD NISP security cognizance as approved when the first set of items 1-4 occur as follows:

1. The covered individual (i.e., cleared employee) notifies the cleared contractor (e.g., Facility Security Officer or assigned designee) before foreign travel. If notification does not occur in advance, the covered individual must notify the cleared contractor as soon as possible after the travel occurs, not to exceed 5 business days;
2. The covered individual submits a complete travel itinerary to the cleared contractor and the cleared contractor reports the travel prior to the unofficial foreign travel as described;
3. The cleared contractor provides the covered individual with the NCSC “Safe Travels” resource for review: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf;
4. The cleared contractor coordinates with a DCSA Counterintelligence Special Agent (CISA) for appropriate pre-foreign travel briefings when the covered individual is traveling to a foreign country listed in the Director of National Intelligence’s Worldwide Threat Assessment of the U.S. Intelligence Community which is available at: <https://www.dni.gov/index.php/newsroom/congressional-testimonies>.

Unofficial Foreign Travel (SEAD-3, F.1.b)

Required for: All Covered Individuals

Additionally, the cleared contractor (FSO or assigned designee) must follow the following guidance:

- ✓ Use travel resources to help inform and advise the covered individual of travel risk. If the covered individual is traveling to a foreign country on the Department of State Travel Advisories List, then cleared contractor should provide information from this advisory to the covered individual.
<https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/>
- ✓ Coordinate with DCSA CISA for post-foreign travel debriefings when covered individual reports any contact with foreign intelligence entities or other foreign travel anomalies during the foreign travel event.
- ✓ If submitting reports of aggregated unofficial foreign travel for covered individuals who routinely travel, this reporting period must not exceed 120 days. In this case, the travel is approved if the FSO refers the covered individual to the NCSC “Safe Travels” resource at least annually for review:
https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf
- ✓ Cleared contractor must ensure that any foreign travel conducted by a covered individual who is terminating their relationship with the cleared contractor is reported immediately.

Unofficial Foreign Travel (SEAD-3, F.1.b)

Required for: All Covered Individuals

Additionally, the cleared contractor (FSO or assigned designee) must follow the following guidance:

- ✓ Deviations from submitted travel itinerary must be reported by the covered individual to the cleared contractor (FSO or assigned designee) within five business days of return.
- ✓ Unplanned day trips to Canada or Mexico by persons residing in the U.S. must be reported to the cleared contractor (FSO or assigned designee) within five business days of return.
- ✓ Unofficial foreign travel under emergency circumstances does not require pre-approval, however, the covered individual should advise their FSO of the emergency foreign travel prior to departure. Reporting, consisting of a complete travel itinerary, shall be accomplished within five business days of return.
- ✓ Covered individuals who are employed by the contractor and who reside abroad are required to report all unofficial foreign travel outside of the foreign country in which they reside. If reports of aggregated unofficial foreign travel are submitted for such covered individuals, the reporting period for that covered individual must not exceed 120 days.
- ✓ Unofficial foreign travel that is not reported in advance and does not fall under the above circumstances, shall be reported to the cleared contractor (FSO or assigned designee) as soon as possible after the travel occurs.

Unofficial Foreign Travel (SEAD-3 Appendix A.1 and ISL 2021-02 Table 4)
Required for: All Covered Individuals

Foreign Travel Reports are
submitted through the DISS
Foreign Travel Module

DISS



Subject Summary



Subject Details



Foreign Travel Tab

Foreign Travel Data Elements:

- a. Complete itinerary.
- b. Dates of travel.
- c. Mode of transportation and identity of carriers.
- d. Passport data.
- e. Names and association (business, friend, relative, etc.) of foreign national traveling companions.
- f. Planned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (business, friend, relative, etc.).
- g. Unplanned contacts with foreign governments, companies, or citizens during foreign travel and reason for contact (post-travel reporting).
- h. Name, address, telephone number, and relationship of emergency point of contact.
- i. Unusual or suspicious occurrences during travel, including those of possible security or counterintelligence significance (post-travel reporting).
- j. Any foreign legal or customs incidents encountered (post-travel reporting).

Unofficial Foreign Contacts (SEAD-3, F.2.b)

Required for: All Covered Individuals

Official Contacts -What Doesn't Need to be Reported?

Contact with foreign nationals occurring solely as part of a covered individual's official duties, and absent any bonds of affection or obligation.

Contact with foreign nationals based solely on the obligations incurred as a result of a covered individual residing in a foreign country due to employment (payment of rent, utilities, etc.), and absent any additional bonds of affection or obligation.

Employment by a cleared contractor with foreign affiliations (e.g., FOCI, multinational business structure) only if such continuing associations involve bonds of affection, personal obligation, or intimate contact.

****If an official foreign contact deemed by the cleared contractor (FSO or assigned designee) is determined to be a security concern, an incident report shall be submitted into DISS.**

Unofficial Foreign Contacts (SEAD-3, F.2.b)
Required for: All Covered Individuals

Report the Following:

1. Unofficial contact with a known or suspected foreign intelligence entity. (*Note: FSO should also report this form of contact directly to the local DCSA Counterintelligence Special Agent)
2. Continuing association with known foreign nationals that involves bonds of affection, personal obligation, or intimate contact.
3. Updates regarding continuing association with known foreign nationals if, and when, there is a significant change in the nature of the contact.
4. Any contact with a foreign national involving the exchange of personal information which meets the following criteria:
 - a. The name and nationality of the foreign national are known by the covered individual during or after the exchange of personal information, and
 - b. The nature of the personal information provided by the covered individual to the foreign national is not reasonably expected to be accessible by the general public, nor to be willingly released to the general public by the covered individual, and
 - c. Contact with the foreign national is re-occurring or expected to re-occur.

DCSA Sample Foreign Contact Reporting Exercise

#	Question	If 'Yes'	If 'No'	If 'I Don't Know'
1	Did you have one or more interactions (in an unofficial capacity) with someone who you know or suspect is associated with a foreign intelligence entity?	Report contact to FSO	Go to question 2	Discuss with FSO
2	Regardless of the person's nationality (U.S. or foreign), is this relationship a marriage, a legally recognized civil union, or legally recognize domestic partnership?	If you have a TS or "Q" eligibility, report this marriage, union or partnership to your FSO, otherwise go to question 4.	Go to question 3	Discuss with FSO
3	Regardless of the person's nationality (either U.S. or foreign), does this person meet the definition of a cohabitant?	If you have a TS or "Q" eligibility, report this cohabitation to your FSO, otherwise go to question 4.	Go to question 4	Discuss with FSO
4	Is this an adoption of a non-US citizen child or children?	If you have a TS or "Q" eligibility, report this adoption to your FSO, otherwise go to question 5.	Go to question 5	Discuss with FSO
5	Does the person have U.S. citizenship, to include being a dual citizen with U.S citizenship, or are they otherwise designated as a U.S. national?	Do not report this contact or relationship	Go to question 6	Go to question 6
6	Is this a continuing relationship with a known foreign national (regardless of it being an official or unofficial foreign contact) that involves bonds of affection, intimate contact, or personal obligation?	Report this relationship to your FSO	Go to question 7	Go to question 7

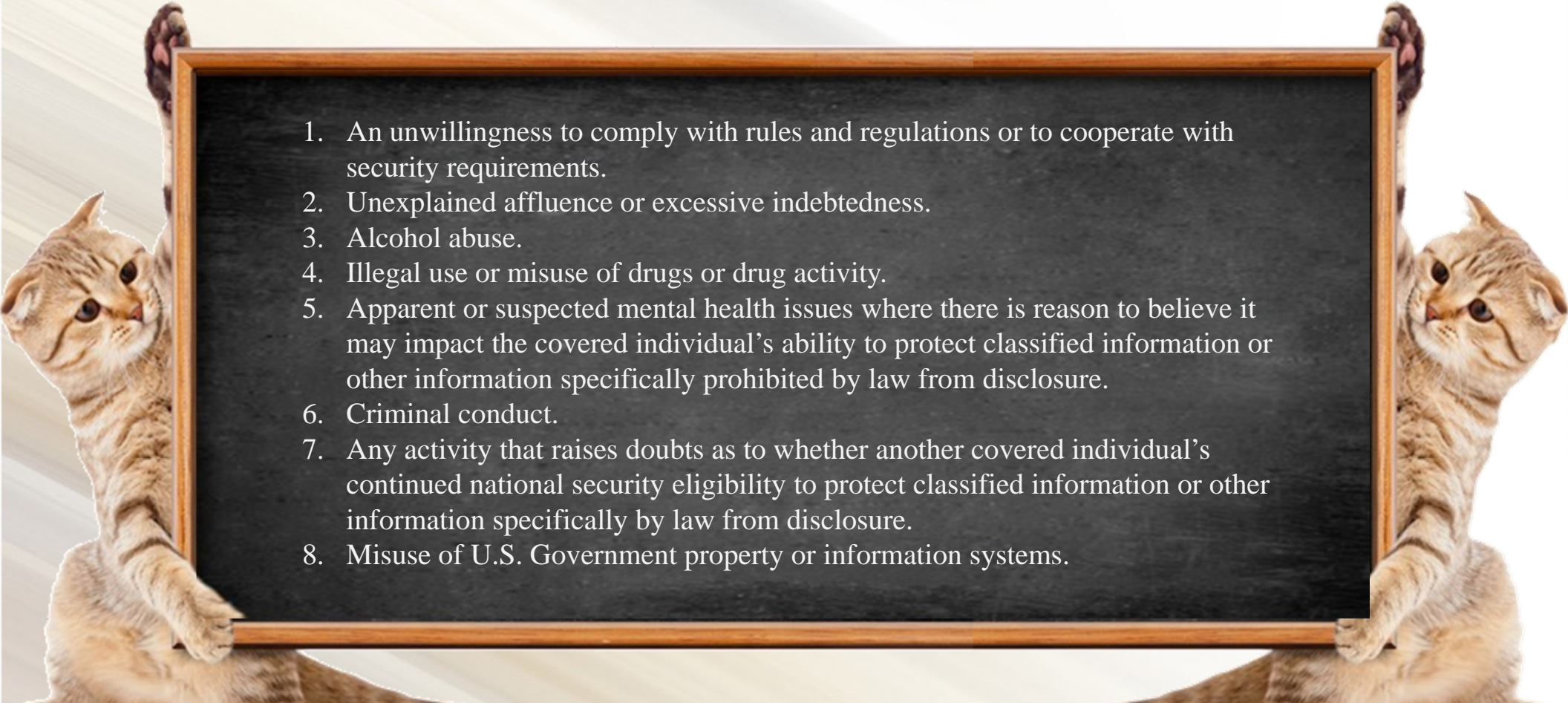
DCSA Sample Foreign Contact Reporting Exercise

#	Question	If 'Yes'	If 'No'	If 'I Don't Know'
7	<p>Does your contact with a foreign national meet the three following criteria:</p> <ul style="list-style-type: none"> a. You know the name and nationality of the foreign national. b. You have provided personal information to the foreign national, meaning information of an intimate or personal nature and that is not reasonably expected to be accessible by the general public, nor that you would willingly release to the general public. This does not include information exchanged during Commercial Transactions, Personable Social, or Professional Interaction c. Contact with the foreign national is re-occurring or expected to re-occur due to the development of an acquaintanceship that extends beyond typical public interaction. 	Report contact to FSO	Go to question 8	Discuss with FSO
8	Is this person a roommate and also a foreign national with whom you've co-occupied a residence with for more than 30 days?	Report contact to FSO	See paragraph below	Discuss with FSO

DCSA created this exercise using the content of the SEAD-3 and ISL 2021-02 documents, but it is not intended to supersede or be a substitute for those documents. If, after answering all 9 of the above questions in the exercise, it still is not clear as to whether the contact or relationship should be reported, the FSO will need to research further guidance.

https://www.dcsa.mil/Portals/91/Documents/IS/DISS/FINAL_SEAD%203%20Contact%20and%20Relationship%20Reporting%20Exercise.pdf

Reportable Actions by Others (SEAD-3, F.3)
Required for: All Covered Individuals

- 
- Two ginger cats are positioned on either side of a rectangular chalkboard with a wooden frame. The cats are standing on their hind legs, with their front paws resting on the top corners of the frame. They are looking towards the camera with a curious expression. The chalkboard is dark and contains a numbered list of eight items.
1. An unwillingness to comply with rules and regulations or to cooperate with security requirements.
 2. Unexplained affluence or excessive indebtedness.
 3. Alcohol abuse.
 4. Illegal use or misuse of drugs or drug activity.
 5. Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information or other information specifically prohibited by law from disclosure.
 6. Criminal conduct.
 7. Any activity that raises doubts as to whether another covered individual's continued national security eligibility to protect classified information or other information specifically by law from disclosure.
 8. Misuse of U.S. Government property or information systems.

Foreign Activities (SEAD-3, G.1 and H.1) Reporting Varies by Eligibility

Confidential, Secret & 'L'

1. Application for and receipt of foreign citizenship.
2. Application for, possession, or use of a foreign passport or identity card for travel.

Top Secret & 'Q'

1. All requirements for Confidential, Secret, & 'L'
2. Direct involvement in foreign business.
3. Foreign bank accounts.
4. Ownership of foreign property.
5. Voting in a foreign election.
6. Adoption of non-U.S. citizen children.



Foreign Activities (SEAD-3, G.1 and H.1) Reporting Varies by Eligibility

Confidential, Secret & 'L'

1. Application for and receipt of foreign citizenship.
2. Application for, possession, or use of a foreign passport or identity card for travel.

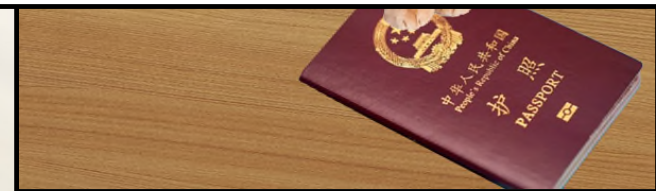
Top Secret & 'Q'

1. All requirements for Confidential, Secret, & 'L'
2. Direct involvement in foreign business.
3. Foreign bank accounts.
4. Ownership of foreign property.
5. Voting in a foreign election.
6. Adoption of non-U.S. citizen children.



SEAD-3, Appendix A Data Elements for Reporting

- a. Location
- b. Estimated Value
- c. Balance Due
- d. Purpose and use of property
- e. How acquired



Other Reportable Activities (SEAD-3, G.2 and H.2) Reporting Varies by Eligibility

Confidential, Secret & 'L'

1. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.
2. Media contacts, other than for official purposes, where media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.
3. Arrests.
4. Bankruptcy or over 120 days delinquent on any debt.
5. Alcohol and drug-related treatment.

Top Secret & 'Q'

1. All requirements for Confidential, Secret, & 'L'
2. Financial Anomalies: Including, but not limited to, garnishments or any unusual infusion of assets of \$10,000 or greater such as an inheritance, winnings, or similar financial gain.
3. Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.
4. Cohabitant(s).
5. Marriage.



Other Reportable Activities (SEAD-3, G.2 and H.2) Reporting Varies by Eligibility

Note from: www.dcsa.mil/mc/isd/NISPOM-Rule/

An “unusual infusion” is an unexpected gain (either monetary or something of monetary value) that is not intended to legally compensate you for a corresponding loss or sale of something. For example, an insurance payment of \$50,000 to cover flood damage to your house is not reportable as an “unusual” infusion because this is a “usual” occurrence given the circumstances of the flood and the corresponding insurance claim. Likewise, properly documented compensation resulting from the sale of personal assets (at a reasonable valuation) or receiving a bonus from your employer in recognition of the value of your performance do not constitute an “unusual” influx since this is simply transferring something of value that you already legally possess into monetary value.

Top Secret & ‘Q’

1. All requirements for Confidential, Secret, & ‘L’
2. Financial Anomalies: Including, but not limited to, garnishments or any unusual infusion of assets of \$10,000 or greater such as an inheritance, winnings, or similar financial gain.
3. Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.
4. Cohabitant(s).
5. Marriage.



Additional Reporting Considerations

From ISL 2021-02, Page 2, Footnotes 2 & 3

This ISL does not provide guidance or clarification on whether to report use of cannabidiol products (also known as CBD products). As a reminder, the U.S. Food and Drug Administration does not determine or certify the tetrahydrocannabinol (THC) concentration of commercially available hemp products, such as CBD. These products may contain appreciable levels of THC, yet omit any reference to THC on the product label or also list an inaccurate THC concentration. Packaging labels cannot be relied upon to disclose if the product contains THC concentrations that could cause a urinalysis result that indicates THC use. A urinalysis result indicating illegal use of drugs may result in adverse action that may impact an individual's security clearance eligibility.

This ISL does not provide guidance or clarification whether to report all willful and direct financial investments or holdings in companies that purchase, manufacture, cultivate, traffic, produce, transfer, shop, receive, handle, or sell schedule I substances (e.g., marijuana) as defined by 21 U.S. Code part 812 within the United States.



DEPARTMENT OF DEFENSE
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
27130 Telegraph Road, Quantico, VA 22134

INDUSTRIAL SECURITY LETTER

Industrial security letters (ISLs) are issued as necessary to inform cleared contractors, Government contracting activities, and DoD Components of developments relating to the National Industrial Security Program. The contents of these letters are for information and clarification of existing policy and requirements. These ISLs only pertain to those entities for whom the Department of Defense is the Cognizant Security Agency. Suggestions for Industrial Security Letters are appreciated and should be submitted to the local Defense Counterintelligence and Security Agency industrial security office. Inquiries concerning specific information in ISLs should be addressed to the local DCSA industrial security office.

ISL 2021-02

August 12, 2021

On February 24, 2021, the rule at 32 CFR part 117, "National Industrial Security Program Operating Manual (NISPOM)" became effective. The rule provides that contractors must implement changes no later than 6-months from the effective date of the published rule, which is August 24, 2021 ("implementation date"). However, DoD has processed an amendment to the NISPOM rule to extend the compliance date solely for reporting and pre-approval of foreign travel reporting until no later than 18 months from the effective date of the rule for those contractors under DoD security cognizance.

CLARIFICATION AND GUIDANCE ON REPORTABLE ACTIVITIES (NISPOM rule, § 117.8(a) and § 117.8(c)(1)). This ISL provides guidance to contractors and covered individuals on the submission of adverse information and the reporting requirements of SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position."¹

If a government contracting activity's (GCA) contract requires additional reporting above the baseline 32 CFR part 117, NISPOM, the contractor should consult with the GCA on when and where to submit such reports.

Covered individuals. In the context of the NISPOM's inclusion of SEAD 3 implementation and this ISL, "covered individuals" refers only to those contractor personnel who have been granted eligibility for access to classified information through the NISP, or are in the process of a determination for eligibility for access to classified information through the NISP. (32 CFR, part 117, Preamble, page 83303). Also, cleared employees are defined in the rule at 32 CFR § 117.3(b).

Uncleared personnel who are subject to SEAD 3 reporting requirements due solely to their occupancy of a "sensitive position" as defined in SEAD 3, D.12., are not covered by the NISP or this ISL and should contact their Government customer for appropriate guidance concerning their SEAD 3 reporting responsibilities.

Nothing in this ISL alters or supersedes the text of the published NISPOM final rule, 32 CFR part 117. This ISL also cancels, incorporates, and rescinds ISL 2011-04, which addressed and provided adverse information reporting examples.

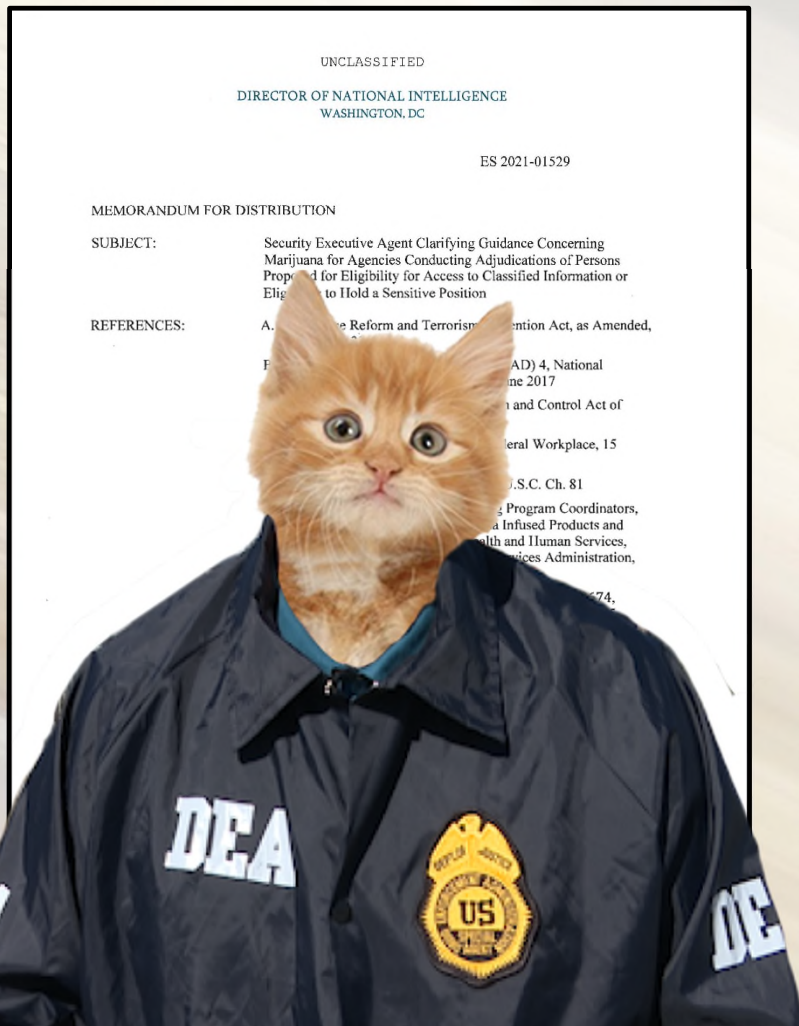
¹ SEAD 3 is located at: <https://www.dau.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-42.pdf>

Additional Reporting Considerations

From Security Executive Agent Memorandum ES2021-01529:


“Regarding CBD products, agencies should be aware that using these cannabis derivatives may be relevant to adjudications in accordance with SEAD-4. Products labeled as hemp-derived that contain greater than 0.3% THC continue to meet the legal definition of marijuana, and therefore remain illegal to use under federal law and policy. Additionally, agencies should be aware that the FDA does not certify levels of THC in CBD products, so the percentage of THC cannot be guaranteed, thus posing a concern pertaining to the use of a CBD product under federal law. Using these products may result in a positive drug test. A positive drug test will raise a security concern that will need to be mitigated.”

“Agencies should note that an adjudicative determination for an individual's eligibility for access to classified information, or eligibility to hold a sensitive position, may be impacted negatively should that individual knowingly and directly invest in stocks or business ventures that specifically pertain to marijuana growers and retailers while the cultivation and distribution of marijuana remains illegal under the Controlled Substances Act.”



Standard Practice Procedures

Current Requirements



32 CFR 117.7(e) requires that contractors prepare written procedures when the CSA determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information, and in accordance with additional Cognizant Security Agency-provided guidance, as applicable.

ISL 2021-02 has identified that the Cognizant Security Agency (DCSA) requires contractors to have a written plan/standard practice procedures (SPP) in place for implementation of SEAD-3 reporting requirements. This written plan/SPP must be available for review during scheduled assessments. DCSA started incorporating the assessment of compliance with SEAD-3 reporting requirements on March 1, 2022.

Current Requirements

ISL 2021-02 requires that the contractor's SPP will, at a minimum, establish the necessary processes and procedures to inform their cleared contractor personnel on reporting requirements related to SEAD-3 and the requirements for adverse information reporting as directed by the NISPOM rule at section 117.8(c)(1).

The SPP will also include processes and procedures that address:

How the contractor receives, processes, and manages the required reports from covered individuals as identified in this ISL.

How these processes and procedures are to be implemented within the cleared contractor facility.

How a covered individual will alert the cleared contractor (FSO or assigned designee) of the reportable actions concerning other covered individuals. (SEAD-3, F.3.)

Unofficial Foreign Travel reporting should also be added to the SPP.

Sample SPP

Quick thought.... You may have to consider reporting requirements for individuals that aren't actively employed by your company.

32 CFR 117.10(f) still allows for processing personnel for investigations prior to the start of their employment. However, the fact that they are not an employee doesn't alleviate you from ensuring that the individual is fulfilling their reporting requirements while their investigation is processing.

Recommendation: add wording to any pre-employment Letter of Intent to ensure individuals understand this additional requirement.



LETTER OF INTENT FOR CLASSIFIED ACCESS PROCESSING

1. Name (Last, First)	2. Contract Name or Number

By initialing and signing below, this letter serves as notice of my intent to accept employment with [company] to perform services in support of the contract identified in Block (2).

Initials _____ I understand that this form may be submitted to the Department of Defense as proof of my intent to perform services on the contract identified in Block (2) of this form. I agree that I will be ready to accept employment with [company] within 45 days of being granted eligibility for the required classified access.

Initials _____ I understand that the applied for position requires the completion of a background investigation consistent with Department of Defense requirements and an approval by the Department of Defense for classified access at the required level. I further understand that submission of this signed letter may be used as proof of my intended employment for sponsorship of my clearance, the initiation of any applicable background check and the processing of my Electronic Questionnaire for Investigative Process (e-QIP), if applicable.

Initials _____ I understand that the sponsorship of my clearance is subject to my continued processing for employment with [company] and I will immediately notify the company of any changes to this stated intent.

Initials _____ I understand that based on the requirements set forth in 32 CFR Part 117, SEAD-3, and ISL 2021-02, I will be required to review reporting requirements that pertain to individuals that have been submitted for a determination for eligibility for access to classified information. Further, that I will be required to submit information pertaining to these requirements to the company during the course of my investigation, to include information that adversely reflects on the integrity or character of myself or any other cleared individual, that suggests that the ability to safeguard classified information may be impaired, that access to classified information clearly may not be in the interest of national security, or if an individual constitutes an insider threat.

Signature _____ Date _____

Signing this form is meant to serve purely as proof of intent that the applicant seeks to perform services as an employee of [company] on the designated contract. Signature on this form does not legally bind applicant to employment or place additional obligations upon applicant outside of the items listed in the main section of this form. Further, submission of this form or processing applicant for a clearance does not create a binding obligation for [company] to hire applicant. Formal employment will be processed through a standard Employment Agreement.

A Template is Just a Template

The following is a potential template for an organization's Standard Practices and Procedures.

Please remember that anyone using a template for a company's program should thoroughly review all sections prior to the implementation of any of the procedures to ensure that it meets any unique requirements of the individual organization.



INDUSTRIAL SECURITY STANDARD PRACTICES AND PROCEDURES

Ver.240731

Senior Management Official – Program Endorsement

Our organization has entered into a Security Agreement with the Department of Defense in order to have access to information that has been classified due to its importance to our nation's defense.

Some of our programs and activities are vital parts of the defense and security systems of the United States. All of us - both management and individual employees - are responsible for properly safeguarding the classified information entrusted to our care.

Our Standard Practice Procedures (SPP) conforms to the security requirements set forth by 32 CFR Part 117, the National Industrial Security Program (NISP). The purpose of our SPP is to provide our personnel with guidelines for meeting NISP requirements as they relate to the type of work we do. This document should also serve as an easy reference when questions about security arise. Questions relating to this plan should be directed to the Facility Security Officer. I fully support our organization's participation and compliance with meeting the requirements of the NISP. All of us have an obligation to ensure that our security practices contribute to the security of our nation's classified defense information.

Senior Management Official

Table of Contents

PART A – SECURITY PROGRAM STANDARD PRACTICES AND PROCEDURES	4
1. PURPOSE	4
2. COVERED INDIVIDUALS	4
3. RESPONSIBILITY	4
4. GRADUATED SCALE OF DISCIPLINE	4
PART B – TRAINING AND REPORTING STANDARDS FOR CLEARED PERSONNEL	5
1. TRAINING	5
2. REPORTING REQUIREMENTS TRAINING	5
3. INITIAL TRAINING	5
4. ANNUAL REFRESHER TRAINING	6
5. ADDITIONAL TRAINING	6
6. ADVERSE INFORMATION REPORTING	6
7. UNOFFICIAL FOREIGN TRAVEL REPORTING	6
8. ADDITIONAL INCIDENTS OR ACTIONS	7
9. PERSONNEL ONBOARDING AND CLEARANCE PROCESSING	7
PART C – CLASSIFIED MATERIAL SAFEGUARDING	8
1. SAFEGUARDING	8
2. CLASSIFIED STORAGE	8
3. PRODUCING CLASSIFIED MATERIAL	9
4. TRANSMISSION OF CLASSIFIED INFORMATION OR MATERIAL	9
5. REPRODUCTION OF CLASSIFIED MATERIAL	9
6. DESTRUCTION OF CLASSIFIED MATERIAL	9
7. RESTRICTED AREA	10
8. END-OF-DAY SECURITY CHECKS	11
ATTACHMENT 1: GRADUATED SCALE OF DISCIPLINARY ACTIONS	12
ATTACHMENT 2: INFORMATION REPORTING FLOWCHART	13
ATTACHMENT 3: FOREIGN TRAVEL REPORTING AND ADVISEMENT	14
ATTACHMENT 4: PERSONNEL CLEARANCE PROCESSING FLOWCHART	15
ATTACHMENT 5: RESTRICTED AREA FLOWCHART	17
ATTACHMENT 6: CLOSE RESTRICTED AREA FLOWCHART	18

PART A – SECURITY PROGRAM STANDARD PRACTICES AND PROCEDURES

1. **PURPOSE.** The Standard Practices and Procedures (SPP) provides the structure for organizational compliance with the requirements set forth in 32 CFR Part 117. It further contains processes for meeting guidelines set forth in Industrial Security Letter (ISL) 2021-02 for implementation of the reporting requirements established by 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 all listed guidances and the Code of Federal Regulations is necessary for effective safeguarding of classified programs and materials, as well as the 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). Additional 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.** A Facility Security Officer (FSO) has been appointed by the organization's Senior Management Official (SMO) 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. **GRADUATED SCALE OF DISCIPLINE.** The organization maintains a discipline matrix in accordance with 32 CFR 117.8(e)(2), which will be utilized in the event of employee security violations or negligence in the handling of classified information. The graduated scale is provided in ATTACHMENT 1.

PART B – TRAINING AND REPORTING STANDARDS FOR CLEARED PERSONNEL

1. **TRAINING.** All Covered Individuals will be provided initial and annual training which sufficiently covers requirements for personnel who receive access to classified material. Additional training may be directed by the FSO on a case-by-case basis to meet additional requirements based on program-specific or situation-specific conditions.

2. **REPORTING REQUIREMENTS TRAINING.** Training covering adverse information reporting will be provided to all personnel defined in A.2, 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.

3. **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. **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.

5. **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.

6. **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.

7. **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.

8. 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.

9. PERSONNEL ONBOARDING AND CLEARANCE PROCESSING. All new personnel requiring access to classified information (employee or consultant) will be processed in accordance with the Personnel Clearance Processing Flowchart (ATTACHMENT 4).

PART C – CLASSIFIED MATERIAL SAFEGUARDING

1. SAFEGUARDING. The organization has been approved to receive and store classified material. All classified materials will be maintained, utilized, stored, transmitted, and destroyed in compliance with all relevant guidances and regulations. The FSO maintains the responsibility for maintaining awareness of updated requirements for safeguarding and will amend the SPP or other policies as necessary.

The organization has been approved for storage at the SECRET level. No personnel are authorized to request any materials at a higher level.

No classified mail is authorized for transmission to the organization's physical address. All classified mailed to the organization must be directed to the approved mailing address:

NAME
MAILING ADDRESS
CITY, STATE, ZIP

The FSO, or authorized designee, maintains the responsibility for receiving, inventorying, and storing classified materials which are received by the organization. Any individual needing to transport classified material to the organization's facility must contact the FSO prior to any such action, meet all requirements for acting as a courier, and receive approval before any such transport.

2. CLASSIFIED STORAGE. The organization maintains a GSA-Approved Safe for the storage of all classified materials. The FSO, assigned designee(s), and a minimum number of appropriately cleared personnel, with requisite need-to-know, will be granted the combination for the safe. The minimum number of personnel is that number which will allow for daily operations to meet contractual compliance.

The combination for the safe is classified at the same level as the material authorized for storage in the safe. Personnel granted access to the combination will not record or make known such combination to any unauthorized personnel.

The combination will be immediately changed upon the reassignment, transfer, or termination of any person having knowledge of the combination; or when the security clearance granted to any such person is downgraded to a level lower than the category of material stored; or when the clearance of any such person has been administratively terminated, suspended or revoked; or upon compromise or suspected compromise of the container or its combination; or the discovery of the container found unlocked and unattended.

All openings, closings, or checks of the GSA-approved safe will be recorded on an SF-702 form which will be maintained with the safe. A list of responsible persons for the safe will also be provided on the safe, along with contact phone numbers.

Signage will be posted in compliance with 32 CFR 117.15(a)(3)(iii)(B), indicating that persons who enter or depart the facility are subject to an inspection, except under circumstances where the possibility of access to classified material is remote.

3. PRODUCING CLASSIFIED MATERIAL. The organization does not currently possess any automated information systems approved for the creation of classified material. Any personnel needing to produce classified information must first coordinate with the FSO. Any classified materials which are produced must be properly stored in compliance with paragraph 2 of this Part.

4. TRANSMISSION OF CLASSIFIED INFORMATION OR MATERIAL. Classified material may only be removed from the Facility following authorized transmission methods. All classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient.

The following methods are approved for transmission:

- Courier
- U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail, as long as the Waiver of Signature block on the U.S. Postal Service Express Mail Label shall not be completed; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited; and

Personnel needing to transmit/transfer any classified material must coordinate with the FSO prior to taking action.

The electronic transmission of classified material is not authorized.

5. REPRODUCTION OF CLASSIFIED MATERIAL. Classified material may only be reproduced on copy machines that have been approved for the reproduction of classified materials. At this time, the organization does not maintain any authorized copy machines. No personnel will create reproductions of any classified material. Requirements for any reproduction to meet contractual requirements must be directed to the FSO for coordination with appropriate agencies.

Any classified reproduction will be accomplished in compliance with 32 CFR 2001.45(b).

6. DESTRUCTION OF CLASSIFIED MATERIAL. Classified information at the Secret Level that is no longer required for contractual performance must be destroyed or returned to the owning

agency/organization. The destruction of any classified must be coordinated through the FSO. If possible, classified material will be returned to the government owner for final disposition.

If material must be destroyed on-site, it will be done in a manner that meets the requirements of 32 CFR 2001.47. Standard procedure for this will be shredding of any materials followed by burning all shredded material. The FSO, or authorized designee, will maintain control over materials until destruction is complete and will verify that material has been destroyed completely to preclude recognition or reconstruction of the classified information.

7. RESTRICTED AREA. The organization will establish a Restricted Area to provide controlled access during any period in which classified discussions take place or when classified material must be utilized for contract activities. All personnel must note that no open-storage is authorized, and all classified materials must be secured in the GSA-approved safe during any non-working hours, at any time when direct access to the classified material is not required, or when there are no authorized personnel maintaining the Restricted Area. Authorized personnel in this capacity must have both the appropriate level of classified access and need-to-know for the specific classified material.

Personnel will follow the Restricted Area Flowchart (ATTACHMENT 5) prior to any classified discussions, the removal of any classified material from the GSA-approved safe, and upon completion of any activities in order to disestablish the Restricted Area.

- No prohibited devices will be authorized in the Restricted Area when it is active. Prohibited devices are any unauthorized devices/items capable of recording or transmitting information internally or externally (wireless, Bluetooth, RF, etc.) which includes but are not limited to: Cell/Smart phones; Laptops; Tablets; iPads; reading devices (e.g., Kindle, Nook); GPS Devices; fitness trackers/Fitbits and smart watches; MP3 Players; iPods; game consoles; noise-cancelling headphones; two-way radios; and two-way pagers.
- Additional steps will include the disconnect of any landline telephones and powering down any unaccredited computer systems. An inspection of the area should also be conducted to verify that no unauthorized devices or equipment have been added to the room as well as a review of the room's perimeter for listening/monitoring devices or functional issues which could diminish the security of classified activities or discussions (e.g., damage to facility wall). The Restricted Area will not be established if any issues are identified which could prevent the proper safeguarding of classified activities and the authorized person will contact the FSO for further guidance and actions.
- Voices and discussions within the Restricted Area must not be discernable outside of the restricted area. A white noise generator will be used when the Restricted Area is in effect

and personnel must be cognizant of noise levels. This will be tested by having one individual outside of the room, checking to ensure that voices inside of the room are not audible.

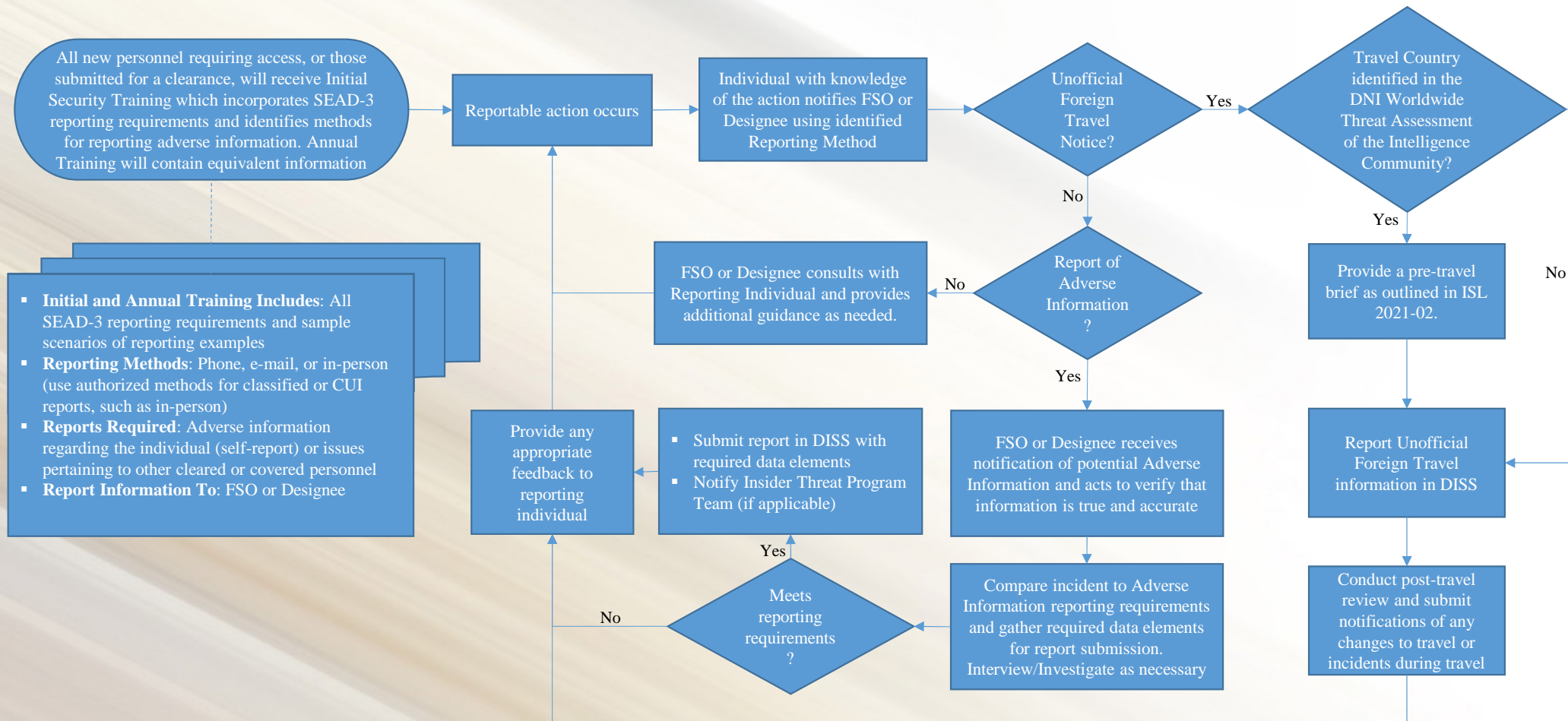
- Classified material shall not be left unattended in the Restricted Area for any amount of time. Classified material must be directly passed from one appropriately cleared and approved person to another. Positive control is physically possessing or maintaining line-of-site control over classified material to preclude unauthorized access. If no authorized person is available to take positive control, all materials must be locked in the classified container. Unattended classified information is a security violation, and any such event must be immediately reported to the FSO.
- Any personnel granted access to the Restricted Area must be verified as being appropriately cleared and possessing a need-to-know. External visitors will be verified through an approved Visitor Authorization Request received through the authorized System of Record (DISS). The FSO has primary responsibility for verifying such requests and communicating approvals to on-site personnel responsible for maintaining the Restricted Area.
- The door to the Restricted Area will be locked to prevent inadvertent access to the area.

8. END-OF-DAY SECURITY CHECKS. An authorized person will complete checks of the storage container at the close of each working day during which access to the container was made. Regardless of access to the container, a check of the container and inventory of classified holdings will be conducted at least weekly and will be documented on the SF-702, Security Container Check Sheet.

ATTACHMENT 1: GRADUATED SCALE OF DISCIPLINARY ACTIONS

MINOR VIOLATIONS (WITHIN A 12-MONTH PERIOD)	
VIOLATION	PENALTIES
FIRST	Individual verbally counseled or issued written reprimand by immediate supervisor and/or Facility Security Officer. Supervisor required to explain security deficiencies to assigned personnel and re-brief them on security requirements.
SECOND	Individual will be given a written reprimand and may be suspended without pay by appropriate next level of management. FSO will conduct a re-briefing of subject individual in presence of direct supervisor or next level management. Depending upon seriousness of offense, attitude of employee, or nature of violation (accidental, deliberate, carelessness, etc.), employee's access may be suspended.
THIRD	Individual given written reprimand, suspension without pay, and may be terminated/separated by appropriate third-level management. FSO will conduct a re-briefing of the subject individual in the presence of third-level management. Depending upon seriousness of offense, attitude of individual, or nature of violation (accidental, deliberate, carelessness, etc.), classified access may be suspended.
MAJOR VIOLATIONS (WITHIN A 12-MONTH PERIOD)	
ANY VIOLATION	Same as the third minor violation.

ATTACHMENT 2: INFORMATION REPORTING FLOWCHART



ATTACHMENT 3: 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:	

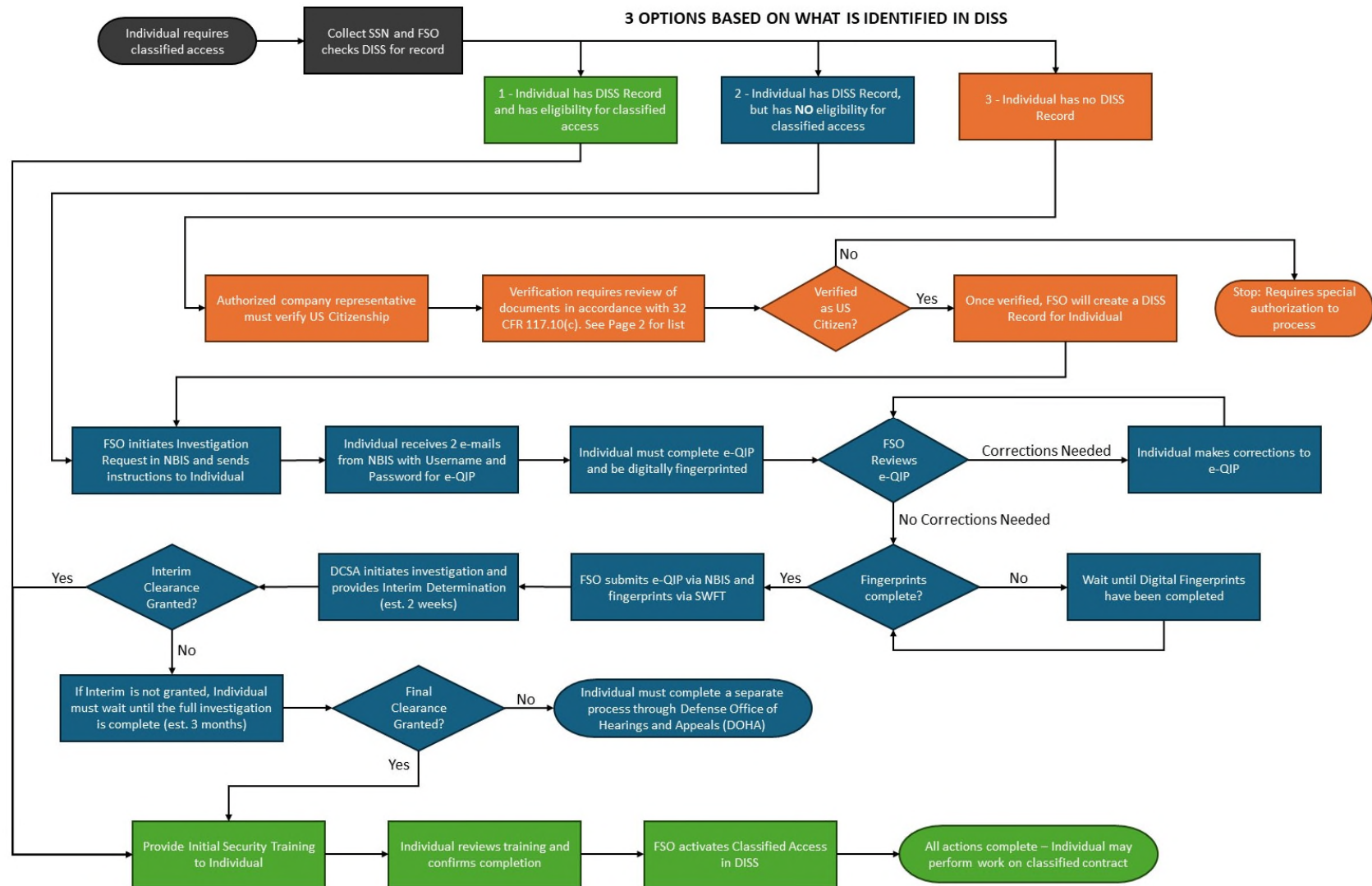
Part 2: Prior to travel. Please review and be aware of the following information.

- ✓ 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/>

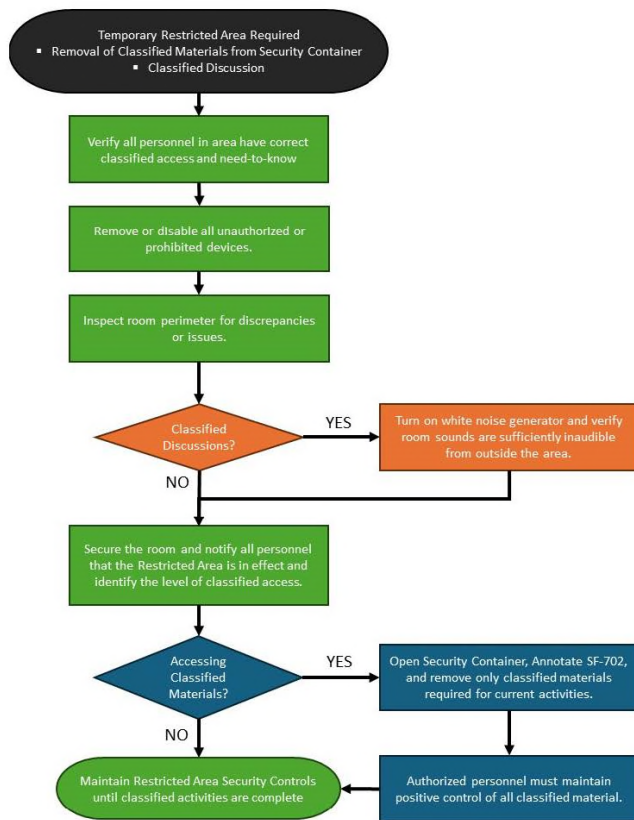
Part 3: Upon the completion of your travel, please notify security if any of the following occurs:

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.)

Personnel Clearance Processing Flowchart – v.240605

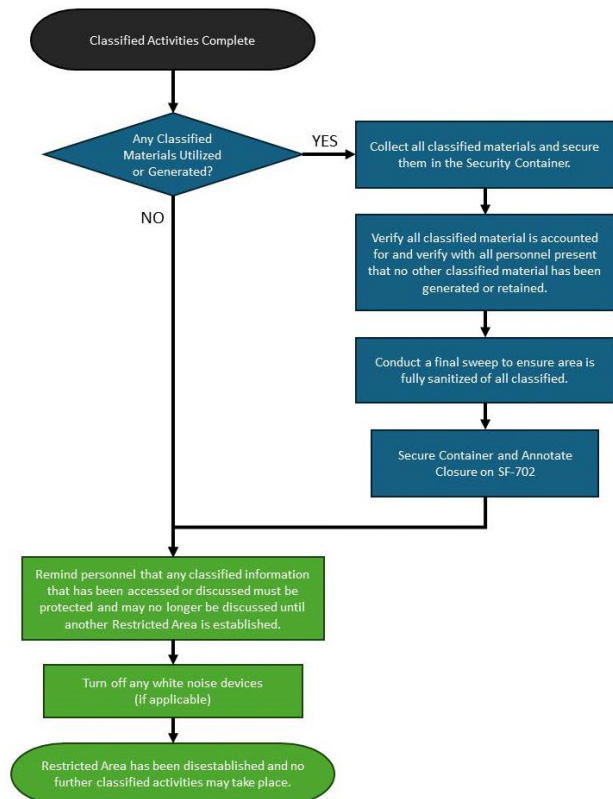


ATTACHMENT 5: RESTRICTED AREA FLOWCHART



17

ATTACHMENT 6: CLOSE RESTRICTED AREA FLOWCHART



Creating Your Own SPP - Considerations

Start by identifying any restrictions.

Do you have internal company guidelines requiring specific formats?

Do you need to meet certain requirements, such as ISO 9001?

Do you need to include other security aspects, such as cybersecurity?

Are there other agency requirements?... DoE may require a more robust SPP even if DCSA does not.

How often do things change?

Will other individuals have control over specific sections of the Procedures that need to be separated or referenced?

Do the procedures cover a location with a shared services agreement?

Determine Scope:

FCL Level?

Possessing Facility?

Restricted Areas?

Do you need to have sections covering CUI, OPSEC, or any other policies?

Any requirements from your DCSA Industrial Security Rep?



References and Aids

SEAD-3 Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position

<https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf>

SEAD-4 National Security Adjudicative Guidelines

<https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>

DCSA Industrial Security Letter 2021-02

https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL2021-02_SEAD-3.pdf

SEAD-3 Industry Reporting Desktop Aid

https://www.dcsa.mil/Portals/91/Documents/CTP/tools/SEAD3_REPORTING_DESKTOP_AID_FOR_CLEARED_INDUSTRY.pdf

DCSA SEAD-3 Reporting Exercise

https://www.dcsa.mil/Portals/91/Documents/IS/DISS/FINAL_SEAD%203%20Contact%20and%20Relationship%20Reporting%20Exercise.pdf

DCSA SEAD-3 Q&A Panel Webinar (12 Oct 2021)

<https://www.dvidshub.net/video/828612/video-series-5-sead-3-panel-questions-answers>

Questions?



www.kavaliro.com

Providing tailored custom solutions to power business growth and providing opportunities for client and employee success.