

# **SEAD-3 Reporting Requirements**

**Will McEllen, SAPPC, ISP  
Armiger, LLC.  
Industrial Security Consulting and Support**

Security Executive Agent Directive 3 (SEAD-3) went into effect in June of 2017, and, in February of 2021, the Defense Counterintelligence Security Agency (DCSA) released an Industrial Security Letter (ISL 2021-02) which provides additional guidance to all cleared personnel regarding their reporting obligations under SEAD-3.

The following presentation provides an overview of contractor requirements as set forth in SEAD-3 and ISL 2021-02.

Please note that SEAD-3 is only one of the reporting requirements for a covered individual addressed in 32 CFR Part 117. SEAD-3 and ISL 2021-12 are not substitutes for, nor do they cancel existing reporting requirements. Other requirements for cleared individuals still include:

- Adverse Information
- Insider Threat
- Incident Reports
- SF-86 submissions (to include updates)
- Suspicious contacts
- Any other contractual government requirement (e.g., SCI and SAP)

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 cognizant office.

**ISL 2021-02**

On February 24, 2021, the rule at 32 CFR part 117, "National Industrial Security Program (NISPOM)" became effective. The rule provides later than 6-months from the effective date of the publication ("implementation date"). However, DoD has processed compliance date solely for reporting and pre-approval of months from the effective date of the rule for those contractors.

**CLARIFICATION AND GUIDANCE ON REPORTING REQUIREMENTS**  
117.8(a) and § 117.8(c)(1). This ISL provides guidance on the submission of adverse information and the reporting requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.

If a government contracting activity's (GCA) contract requires reporting to 32 CFR part 117, NISPOM, the contractor should consult with the cognizant office.

**Covered individuals.** In the context of the NISPOM and this ISL, "covered individuals" refers only to those individuals who are granted eligibility for access to classified information of a determination for eligibility for access to classified information. (*CFR, part 117, Preamble, page 83303. Also, cfr 32 CFR § 117.3(b).*)

**Uncleared personnel who are subject to SEAD-3 reporting requirements.** Personnel who are not cleared for access to classified information, but who are subject to SEAD-3 reporting requirements, should contact their cognizant office for guidance concerning their SEAD-3 reporting requirements.

Nothing in this ISL alters or supersedes the text of the NISPOM. This ISL also cancels, incorporates, and rescinds ISL 2017-01 information reporting examples.

<sup>1</sup> SEAD 3 is located at: <https://www.dni.gov/files/NCS/CS/documents/SEAD3.pdf>

UNCLASSIFIED

**SECURITY EXECUTIVE AGENT  
DIRECTIVE 3**

**REPORTING REQUIREMENTS FOR PERSONNEL WITH ACCESS TO CLASSIFIED  
INFORMATION OR WHO HOLD A SENSITIVE POSITION**

(EFFECTIVE: 12 JUNE 2017)

**A. AUTHORITY:** The National Security Act of 1947, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, as amended; Executive Order (EO) 10450, *Security Requirements for Government Employment*, as amended; EO 12968, *Access to Classified Information*, as amended; EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*; EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*; Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*; Performance Accountability Council memorandum, *Assignment of Functions Relating to Coverage of Contractor Employee Fitness in the Federal Investigative Standards*, 6 December 2012; and other applicable provisions of law.

**B. PURPOSE:** This Security Executive Agent (SecEA) Directive establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. Nothing in this Directive should be construed to limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation.

**C. APPLICABILITY:** This Directive applies to any executive branch agency or covered individual as defined below.

**D. DEFINITIONS:** As used in this Directive, the following terms have the meanings set forth below:

1. "Agency": Any "Executive agency" as defined in Section 105 of Title 5, United States Code (U.S.C.), including the "military department," as defined in Section 102 of Title 5, U.S.C., and any other entity within the Executive Branch that comes into possession of classified information or has positions designated as sensitive.
2. "Classified national security information" or "classified information": Information that has been determined pursuant to EO 13526 or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure.
3. "Cohabitant": A person with whom the covered individual resides and shares bonds of affection, obligation, or other commitment, as opposed to a person with whom the covered individual resides for reasons of convenience (e.g. a roommate).
4. "Controlled Substance": Any controlled substance as defined in 21 U.S.C. 802.
5. "Covered individual":

UNCLASSIFIED

## 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

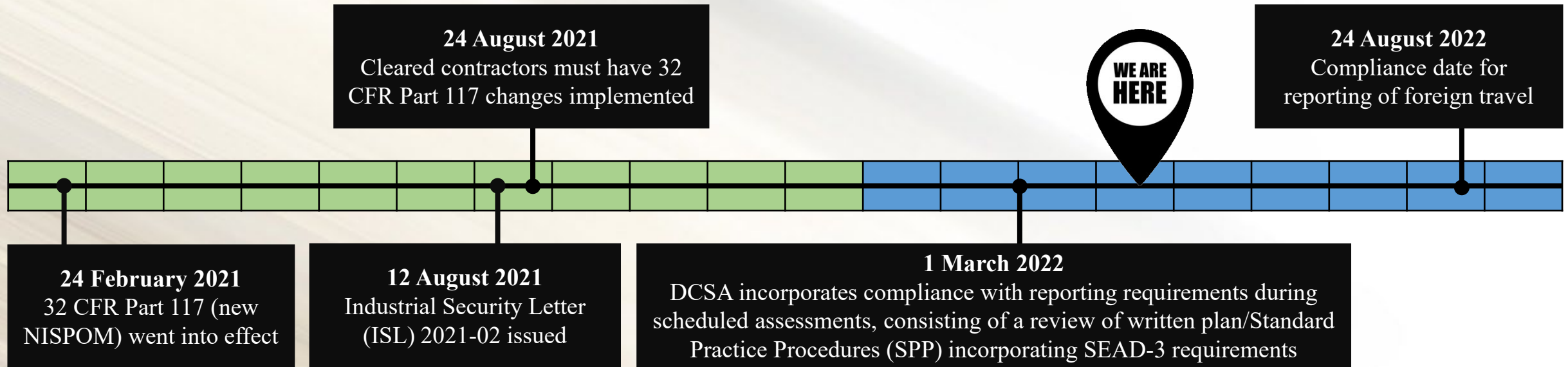
<https://www.cdse.edu/Training/Security-Shorts/Personnel-Security-Shorts/>

- 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

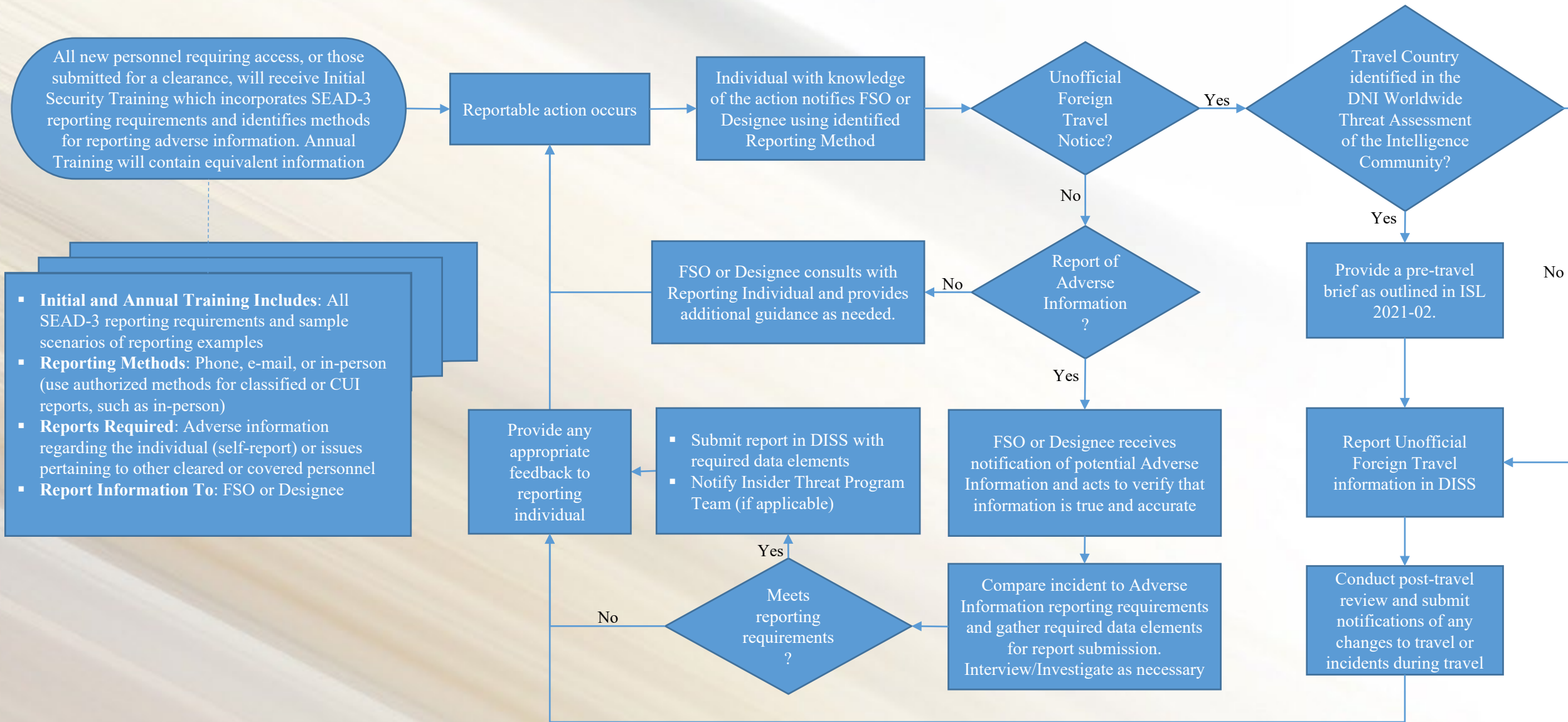
## SEAD-3 Notable Dates and Compliance



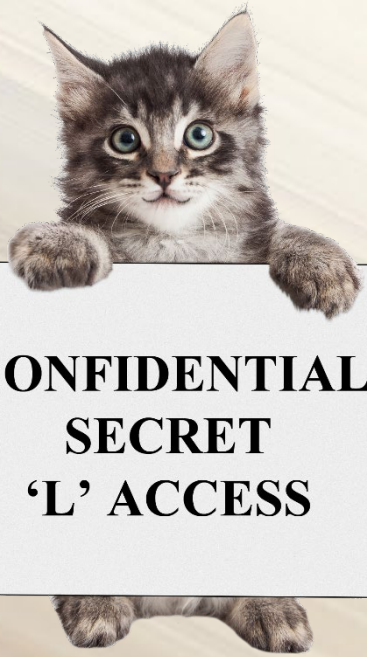
DCSA requires that the contractor's written plan/SPP will, at a minimum, establish the necessary processes and procedures to inform their cleared contractor personnel on reporting requirements related to SEAD-3 and the requirements for adverse information reporting as directed by 32 CFR Part 117.8(c)(1).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



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



**CONFIDENTIAL  
SECRET  
'L' ACCESS**

- Unofficial Foreign Travel
- Unofficial Foreign Contacts
- Behavior & Conduct of Others
- Foreign Affiliation (Citizenship, Passport)
- Media Contact
- Criminal Activity
- Alcohol & Drug Treatment
- Bankruptcy or Financial Issues
- Personal Behavior & Conduct
- Financial Anomalies
- Non-U.S. Adoption
- Marriage
- Cohabitation
- Foreign National Roommate
- Foreign Business
- Foreign Property
- Foreign Bank Accounts



**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
<b>Personal Finance &amp; Business Interests</b>	<p><i>(REMINDER: "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. 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.)</i></p> <p><b>Cryptocurrency.</b> 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"> <li>• Name of cryptocurrency</li> <li>• Exchange host country</li> <li>• Dollar value of the asset</li> </ul>

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) <sup>1,2</sup>	YES See Footnotes	YES See Footnotes	F.1.b.; Appendix A.1, items e, f, h, and as needed g, l, and j	4
Foreign Travel (Unofficial), deviations from submitted travel itinerary <sup>1,2</sup>	YES See Footnotes	YES See Footnotes	F.1.b.1.	4
Foreign Travel (Unofficial), unplanned trips to Canada or Mexico <sup>1,2</sup>	YES See Footnotes	YES See Footnotes	F.1.b.(b)	4
Foreign Travel (Unofficial), emergency circumstances <sup>1,2</sup>	YES See Footnotes	YES See Footnotes	F.1.b.1.(d)	4

<sup>1</sup> 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.

<sup>2</sup> 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](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](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 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).

Foreign Travel Reports are  
submitted through the DISS  
Foreign Travel Module

DISS



Subject Summary

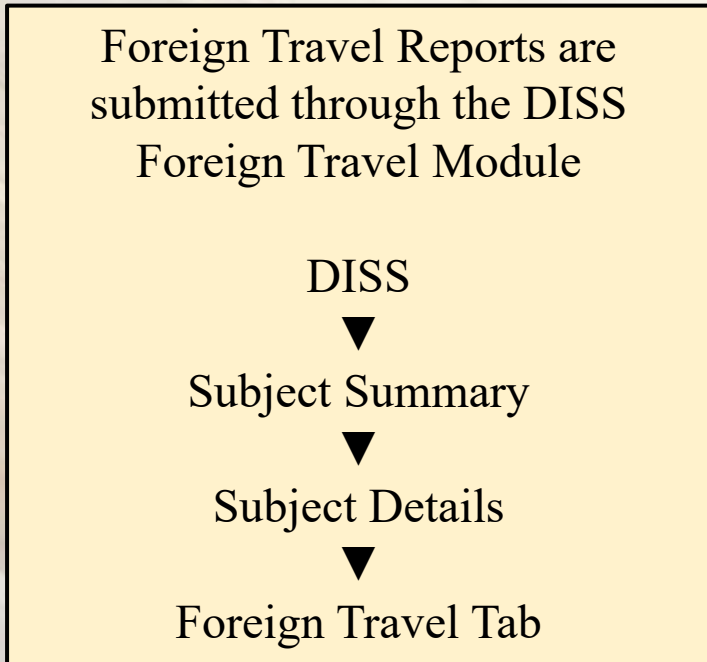


Subject Details



Foreign Travel Tab

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



## Foreign Travel Data Elements:

- a. Complete itinerary.
- b. Dates of travel.
- c. Mode of transport and identity of carriers.
- d. Passport number.
- e. Name of contact (business, friend, relative, etc.) of foreign national.
- 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 experiences during travel, including those of possible security or counterintelligence significance (post-travel reporting).
- j. Any foreign legal incidents encountered (post-travel reporting).

**Don't Forget!  
Foreign Travel  
Reporting  
Starts 24 August**



## **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

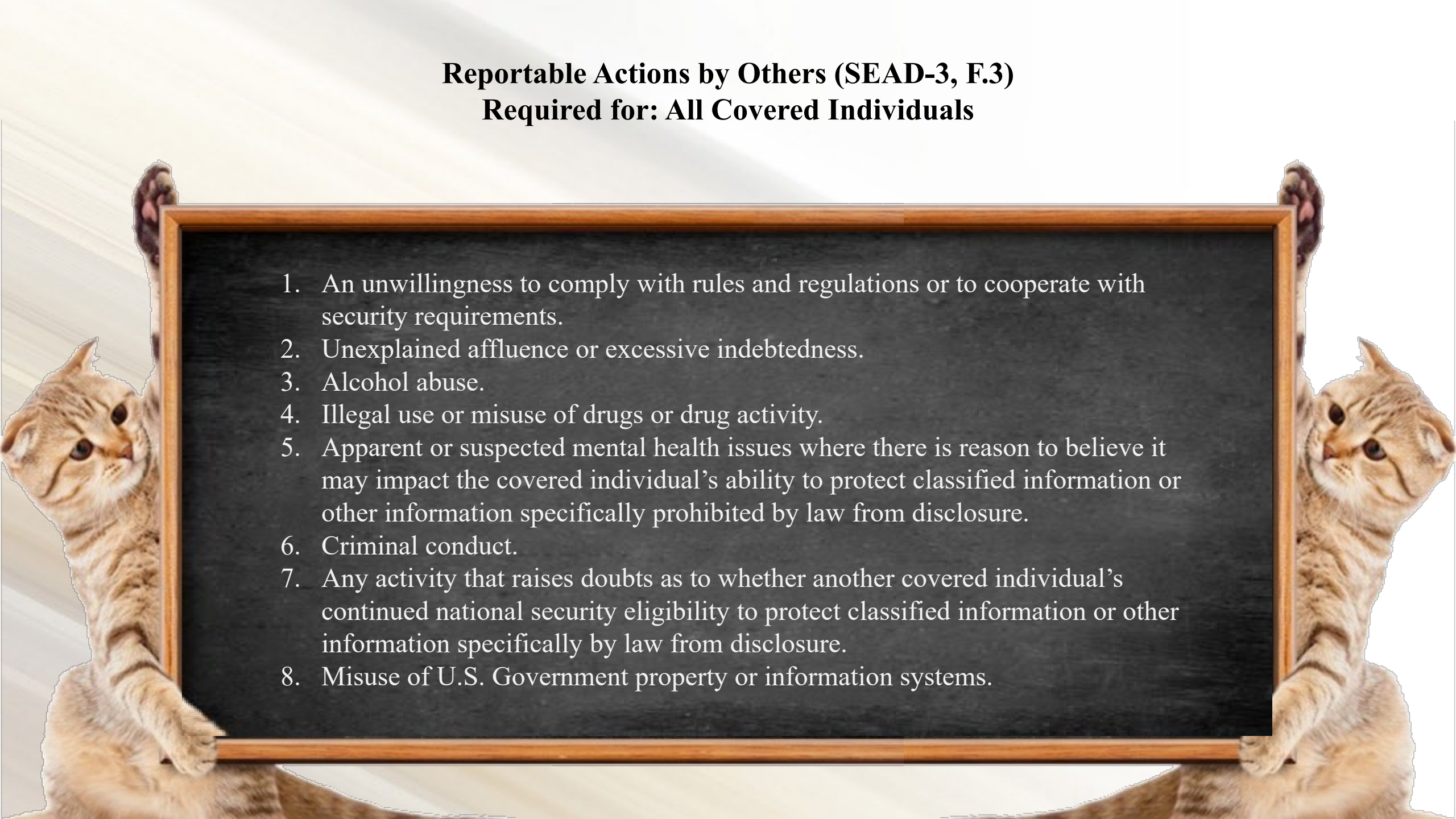
#	Question	If 'Yes'	If 'No'	If 'I Don't Know'
7	<p>Does your contact with a foreign national meet the three following criteria:</p> <ul style="list-style-type: none"> <li>a. You know the name and nationality of the foreign national.</li> <li>b. You have provided personal information to the foreign national, 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</li> <li>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.</li> </ul>	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](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**

- 
- The image features two ginger cats on either side of a blackboard. The cats are standing on their hind legs, holding the corners of a wooden frame that surrounds the blackboard. The blackboard contains a list of eight reportable actions. The background is a light, textured surface with a subtle gradient.
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/](http://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."<sup>1</sup>

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.

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

# Additional Reporting Considerations

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE  
WASHINGTON, DC

ES 2021-01529

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Security Executive Agent Clarifying Guidance Concerning Marijuana for Agencies Conducting Adjudications of Persons Proposed for Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position

- REFERENCES:
- A. Intelligence Reform and Terrorism Prevention Act, as Amended, 50 U.S.C. § 3343
  - B. Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines, 08 June 2017
  - C. Comprehensive Drug Abuse Prevention and Control Act of 1970, 21 U.S.C. § 801 et seq.
  - D. Executive Order 12564, Drug-Free Federal Workplace, 15 September 1986
  - E. Drug-Free Workplace Act of 1988, 41 U.S.C. Ch. 81
  - F. Memorandum to Federal Agency Drug Program Coordinators, Marijuana, Marijuana Oils, Marijuana Infused Products and Hemp Products, Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, 24 July 2019
  - G. Security Executive Agent Memorandum ES 2014-00674, Adherence to Federal Laws Prohibiting Marijuana Use, 25 October 2014
  - H. The National Security Act of 1947, as amended

Pursuant to 50 U.S.C. § 3162a, as the Security Executive Agent (SecEA) for the United States Government (USG), I am responsible for issuing guidelines and instructions to the heads of federal agencies to ensure appropriate uniformity in process relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position, including such matters as investigations, polygraphs, adjudications, and reciprocity. As such, the purpose of this memorandum is to provide clarifying guidance to authorized adjudicative agencies relating to an individual's involvement with marijuana, particularly in response to the increase in the number of state and local governments legalizing or decriminalizing uses of marijuana.

UNCLASSIFIED

## 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.”

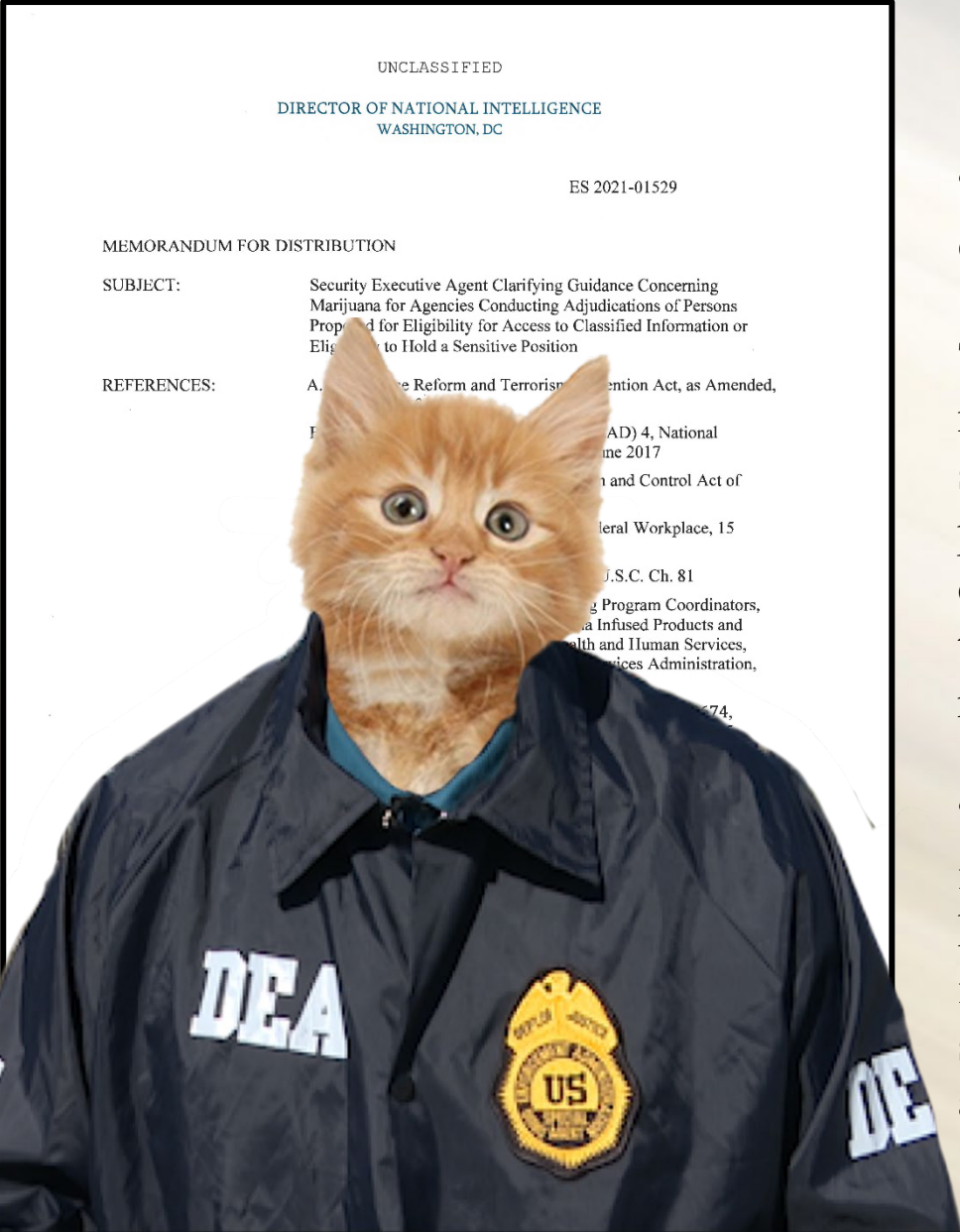
“Agencies should note that an adjudicative determination for an individual's eligibility for access to classified information, or eligibility to hold a sensitive position, may be impacted negatively should that individual knowingly and directly invest in stocks or business ventures that specifically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

# 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.”



## 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](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](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](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?



**Will McEllen, SAPPC, ISP  
Armiger, LLC.**

**Industrial Security Consulting and Support  
will.mcellen@armigerllc.com**