Please note that this sample Standard Practices and Procedures is being provided 'as-is' and anyone who chooses to utilize the procedures identified herein, in part on in whole, must first perform all necessary due diligence to ensure proper compliance with any existing rules, regulations, or guidelines which may apply to their respective Facility or 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

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.

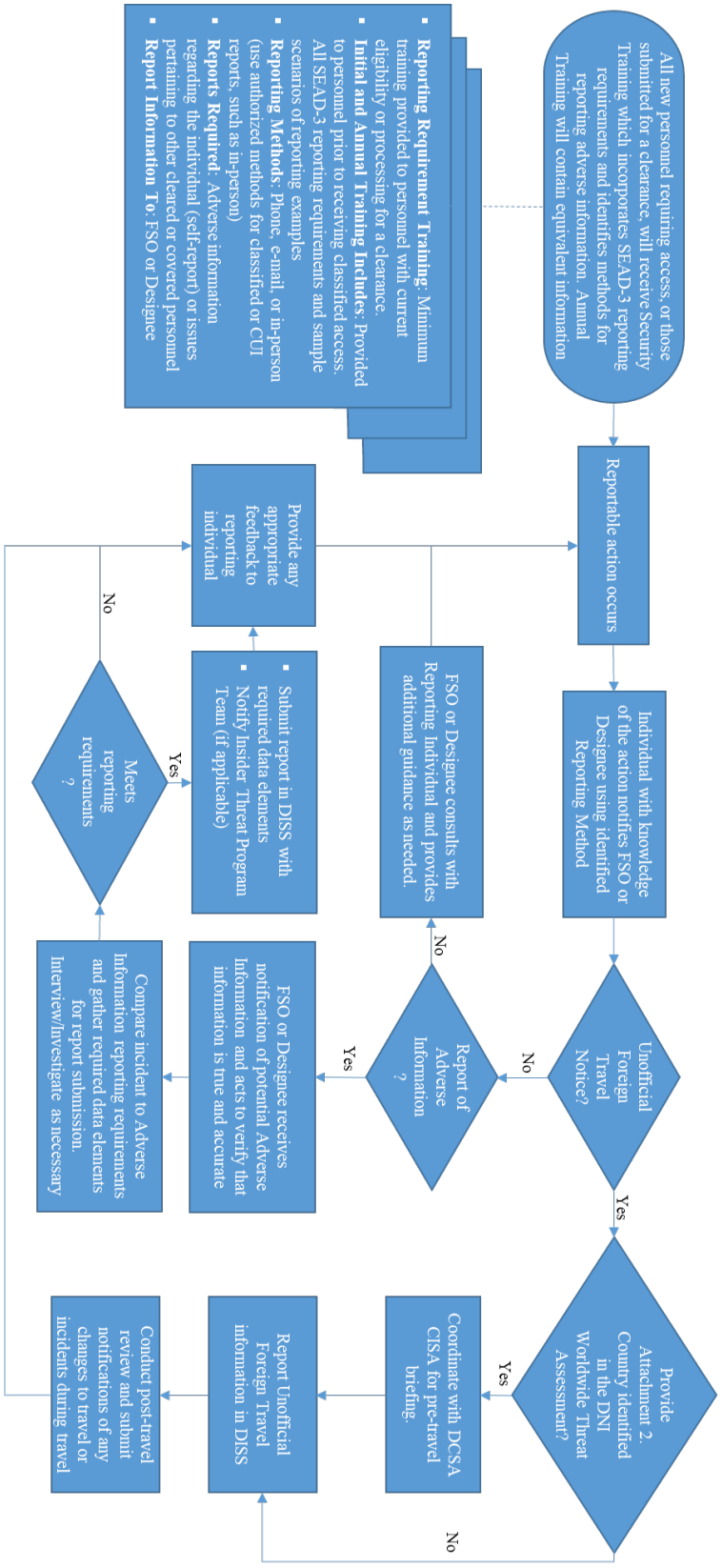
- The door to the Restricted Area will be locked to prevent inadvertent access to the area.

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

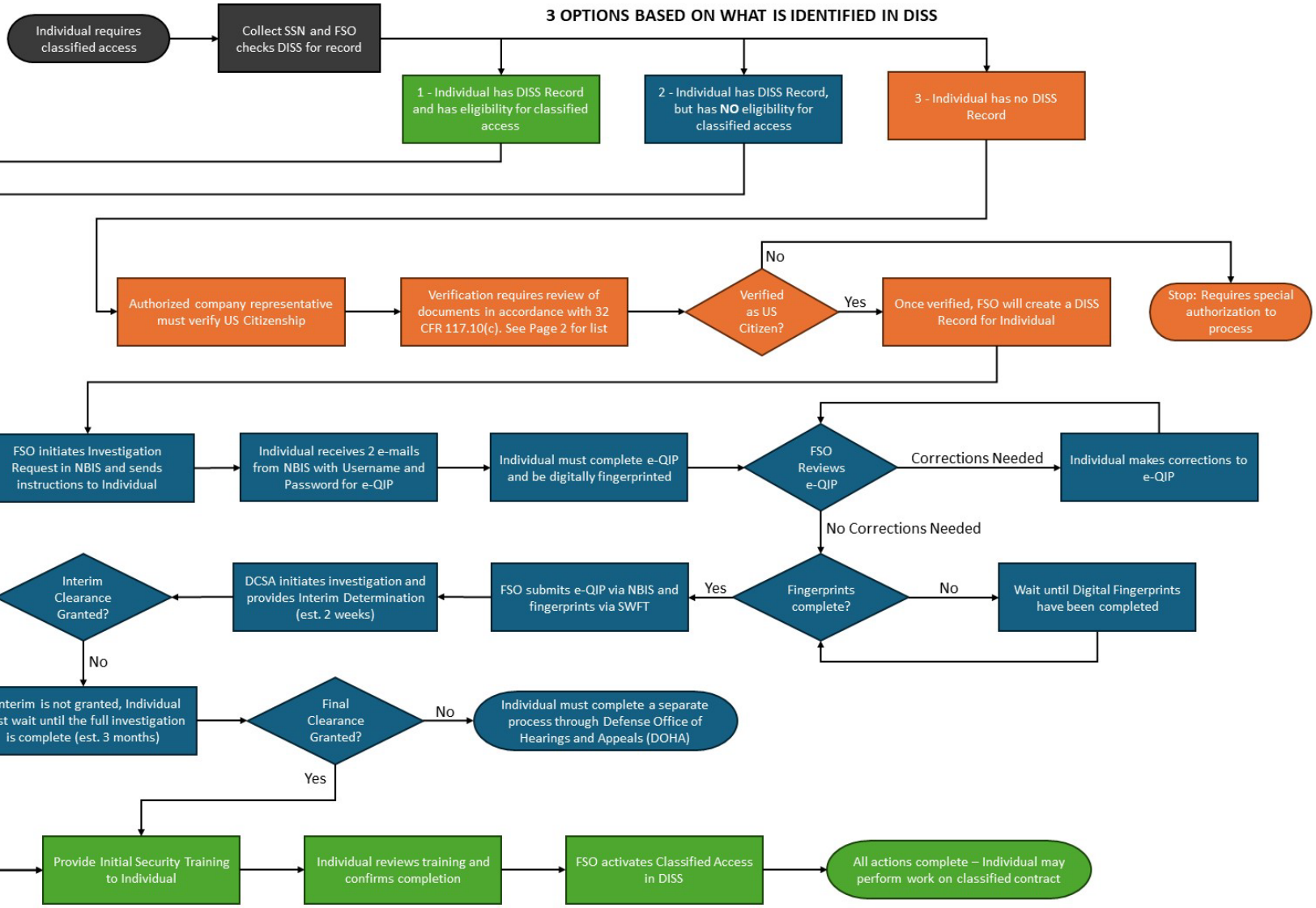
- ✓ Review the Department of State Travel Advisories to determine if any of your travel (including layovers or transfers) will be in a country with an existing advisory. Review any such advisories prior to travel and contact the security office if you have any questions: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

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.)

ATTACHMENT 4: PERSONNEL CLEARANCE PROCESSING FLOWCHART

Personnel Clearance Processing Flowchart – v.240605



Documents for Verifying US Citizenship – established by 32 CFR 117.10(c).

(1) Any document, or its successor, listed in this paragraph is an acceptable document to corroborate U.S. citizenship by birth, including by birth abroad to a U.S. citizen.

(i) A birth certificate certified with the registrar's signature, which bears the raised, embossed, impressed, or multicolored seal of the registrar's office.

(ii) A current or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.

(iii) A Department of State Form FS-240, "Consular Report of Birth Abroad of a Citizen of the United States of America."

(iv) A Department of State Form FS-545 or DS-1350, "Certification of Report of Birth."

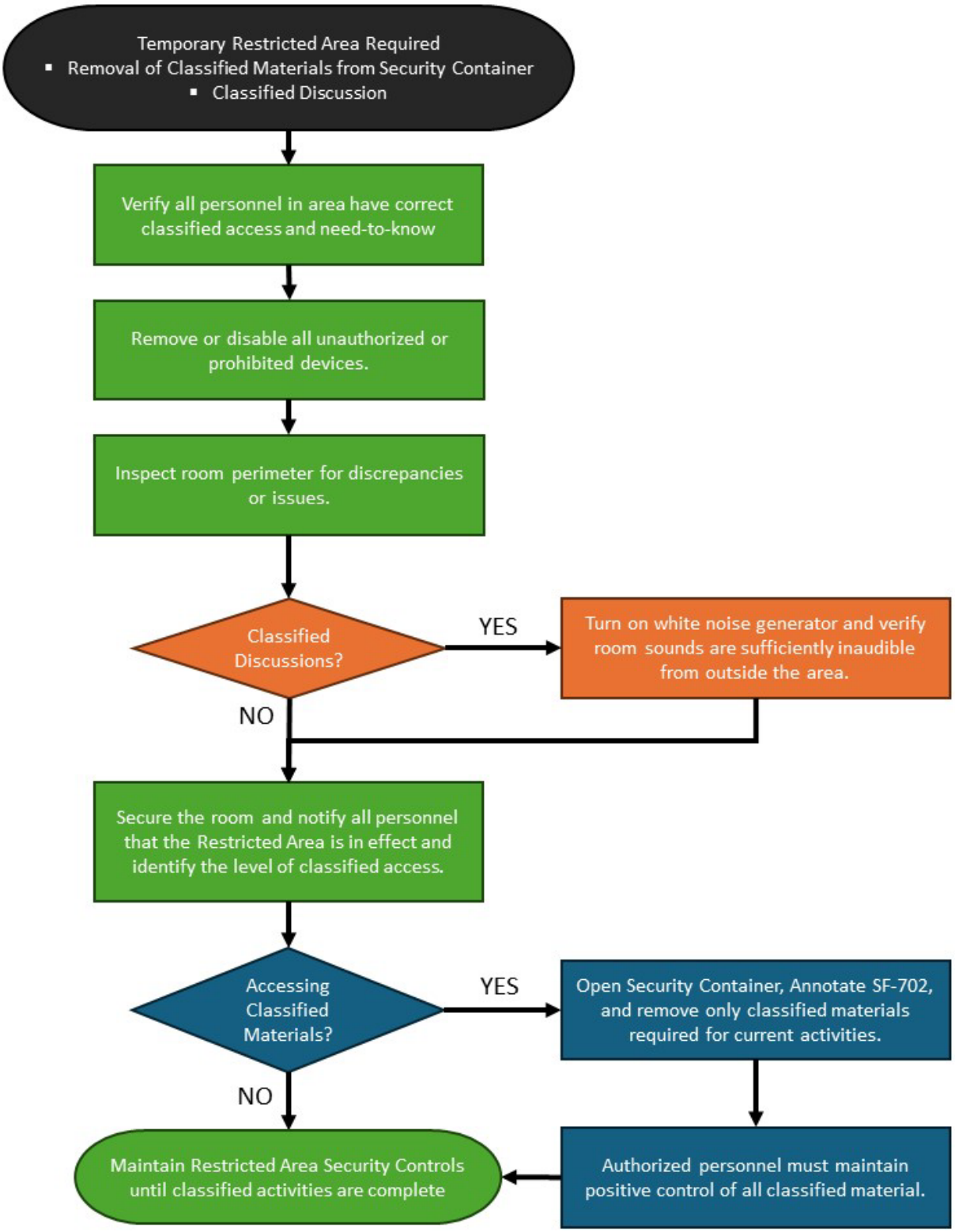
(2) Any document, or its successor, listed in this paragraph is an acceptable document to corroborate U.S. citizenship by certification, naturalization, or birth abroad to a U.S. citizen.

(i) A U.S. Citizenship and Immigration Services Form N-560 or N-561, "Certification of U.S. Citizenship."

(ii) A U.S. Citizenship and Immigration Services Form 550, 551, or 570, "Naturalization Certificate."

(iii) A valid or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.

ATTACHMENT 5: RESTRICTED AREA FLOWCHART



ATTACHMENT 6: CLOSE RESTRICTED AREA FLOWCHART