STANDARD PRACTICES AND PROCEDURES (SPP) POSSESSING

TRUSTEES OF PURDUE UNIVERSITY, THE
2550 Northwestern Ave #1100
West Lafayette, IN 47906
CAGE Code: 6D418

LAST UPDATED: DECEMBER 16, 2024

REVISION #: 2

SMO SIGNATURE _____

FSO SIGNATURE _____

REVISIONS

Version. Number	Date	Section(s)	Description	Director of Security Initials
1	September 18, 2024	New	Initial document	See Title Page
2	December 16, 2024	Foreward	Removed reference to Security Control	ARC
2	December 16, 2024	2	Removed original sections 2.1.a (on Security Control) and 2.2.d (on Assistant FSO)	ARC
2	December 16, 2024	2.2.b	Removed reference to Security Control	ARC
2	December 16, 2024	3.2	Removed reference to Security Control	ARC
2	December 16, 2024	3.2	Removed reference to Addendum A	ARC
2	December 16, 2024	3.3	Removed reference to Security Control	ARC
2	December 16, 2024	3.4	Removed reference to Security Control	ARC
2	December 16, 2024	3.7	Removed reference to Security Control	ARC
2	December 16, 2024	3.9	Removed reference to Security Control	ARC
2	December 16, 2024	4	Removed reference to Security Control	ARC
2	December 16, 2024	5	Removed reference to Security Control	ARC
2	December 16, 2024	6.1.a	Removed reference to Security Control	ARC
2	December 16, 2024	6.1.e	Removed reference to Security Control	ARC
2	December 16, 2024	7.1	Removed reference to Security Control	ARC
2	December 16, 2024	7.2	Removed reference to Security Control	ARC
2	December 16, 2024	7.2.b	Removed reference to Security Control	ARC
2	December 16, 2024	7.2.c	Removed reference to Security Control	ARC

2	December 16, 2024	7.3.a	Removed reference to Security Control	ARC
2	December 16, 2024	7.4	Removed reference to Security Control	ARC
2	December 16, 2024	8.2	Removed reference to Security Control	ARC
2	December 16, 2024	9	Removed reference to Security Control	ARC
2	December 16, 2024	13	Removed reference to Security Control	ARC
2	December 16, 2024	13.2	Removed reference to Security Control	ARC
2	December 16, 2024	16	Removed reference to Security Control	ARC
2	December 16, 2024	17-19	Removed original sections 17-19 pertaining to DISS, NBIS and NISS accounts.	ARC
2	December 16, 2024	17	Removed reference to Security Control	ARC
2	December 16, 2024	17.2	Removed reference to Security Control	ARC
2	December 16, 2024	17	Removed sections (originally 20.3 and 20.4) on modifying, cancelling or entering outgoing and incoming visits in DISS	ARC
2	December 16, 2024	18	Removed heading 18.1, originally 21.1.	ARC
2	December 16, 2024	18	Removed steps for initiating an investigation in NBIS (originally section 21.2), and changed language for the purpose of an investigation from “supporting a contract” to “in accordance with the NISPOM.”	ARC
2	December 16, 2024	19	Removed reference to Security Control	ARC
2	December 16, 2024	19.1	Removed names	ARC
2	December 16, 2024	20.2	Removed reference to Security Control	ARC
2	December 16, 2024	21	Removed original section 24.2	ARC
2	December 16, 2024	21.2	Changed reporting by ITPSO from SMO and DCSA to ITWG	ARC

2	December 16, 2024	21.2	Removed ISSO position	

FOREWORD

Purdue University (sometimes referred to herein as "Purdue" as well as the pronouns "we" and "our" as the context requires) has entered into a Security Agreement with the Department of Defense (DoD) to have access to information that has been classified because of its importance to our Nation's defense. Purdue University fully supports the National Industrial Security Program (NISP), as we have an obligation to ensure that our security practices contribute to the security of our Nation's classified defense information.

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 Practices & Procedures (SPP) conform to the security requirements set forth in the Government Manual, the 32 Code of Federal Regulations Part 117 National Industrial Security Program Operating Manual (NISPOM RULE).

The purpose of our SPP is to provide our Employees with the requirements of this manual as this relates to the type of work we do. This document should also serve as an easy reference when questions about security arise.

The NISPOM RULE is available for review by contacting the Facility Security Officer (FSO) or through ecfr.gov.

1. Introduction

This SPP describes our policies regarding the handling and protection of classified information. This SPP is applicable to all Employees, Subcontractors, Consultants, Vendors, and Visitors to our facility, and is a supplement to the National Industrial Security Program Operating Manual (32 CFR PART 117, NISPOM RULE), which takes precedence in instances of apparent conflict. These practices and procedures also describe our internal operational policies concerning the management of all aspects relating to the NISPOM RULE.

Purdue University participates in the National Industrial Security Program (NISP) to conduct research to support our Nation's security and defense. Purdue University contracts with Department of Defense and Industry partners to conduct this research and may require employees to maintain a clearance up to the Top Secret level.

Additional Specific Operating Procedures (SOP) may be attached as addendums.

2. Facility Information

2.1. Facility Clearance

A Facility Clearance (FCL) is an administrative determination that a facility is eligible for access to classified information or the award of a classified contract. The FCL is valid for access to classified information and allows us to maintain Personnel Security Clearances (PCL's) for our Employees so they can perform on classified contracts. Please reach out to the Security Team (FSO@purdue.edu) if you require specifics relating to our FCL levels and accesses. We do not post these online, or in documented form. Each Employee will receive this information in their initial security briefing and then again during their annual refresher training.

2.2. Key Management Personnel (KMP)

KMP means an entity's senior management official (SMO), facility security officer (FSO), insider threat program senior official (ITPSO), and all other entity officials who either hold majority interest or stock in, or have direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.

2.2.a. Senior Management Official (SMO)

The SMO must do the following: (1) ensure Purdue University maintains a system of security controls in accordance with the requirements of the National Industrial Security Program (NISP); (2) remain fully informed of the facility classified operations; (3) make decisions based on classified threat reporting and their thorough knowledge, understanding and appreciation of the threat information and the potential impacts caused by a loss of classified information; and (4) retain accountability for the management and operations of the facility without delegating that accountability to another Employee.

2.2.b. Facility Security Officer (FSO)

As a result of having an FCL, we agree to adhere to the rules of the NISPOM RULE. As part of the NISPOM RULE, Purdue University has appointed a Facility Security Officer (FSO). Our FSO is a United States citizen, an Employee of Purdue University, and cleared to the level of the FCL. Our FSO will complete all required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM RULE and the related Federal requirements for classified information. The FSO curriculum will be completed within six (6) months of appointment. The FSO or those otherwise performing security duties shall complete security training per the NISPOM RULE "117.12 (d)" and as deemed appropriate by the Cognizant Security Agency (CSA).

2.2.c. Insider Threat Program Senior Official (ITPSO)

The ITPSO must do the following: (1) ensure that there is an executed Insider Threat Program that includes the FSO and other department heads if applicable; (2)discuss the required training for all Employees; (3) Ensure the program has been established to ensure safeguards and resources are in place to provide Purdue University hard working and dedicated workforce with a safe environment to carry out its important mission.

This program is designed to deter, detect, and mitigate actions by insiders who represent a threat to National Security.

2.3. Detailed Threat Report

The current threats pursuant to our line of business mainly consist of cyber breaches, both from individuals, as well as from foreign nations. Both classified and unclassified threat reports can be obtained from the Defense Counterintelligence Security Agency (DCSA). The unclassified version, Targeting US Technologies, can be accessed on DCSA's website. These threat reports will be used to identify threats specific to our business and help identify Company assets that need protection.

2.4. Government Customers

Our Government Customers are responsible for providing us with the appropriate security guidance based on each individual Government Contract. In most cases, this will be done by a DD Form 254. For any inaccuracies or questions on the DD Form 254, we will consult with the Government Customer.

3. Security Education

3.1. Initial Security Briefings

Prior to being granted access to classified information, an Employee/Consultant shall receive an initial security briefing that includes the following:

- Threat awareness security briefing
- Counterintelligence awareness briefing
- An overview of the information security classification system
- Employee reporting obligations and requirements, including insider threat
- Security procedures and duties applicable to the Employee's position

3.2. Insider Threat Training

The ITPSO will ensure that Company program personnel assigned insider threat program responsibilities and all other cleared Employees complete training consistent with applicable DCSA provided guidance, which shall include:

(1) Insider Threat Awareness INT 101.16 (Required)
(2) Establishing an Insider Threat Program INT 122.16 (Required)
(3) Insider Threat Mitigation Response INT 210.16 (Required)
(4) Counterintelligence Awareness and Security Brief CI112.16 (Required)
(5) Insider Threat Privacy and Civil Liberties INT 260.16 (Required)
(6) Developing A Multidisciplinary Threat Capability (INT 201.16) (Highly recommended)

Our ITPSO will provide insider threat awareness training to all new Employees/Consultants before granting access to classified information and existing cleared Employees on an annual basis. Our training addresses the current and potential threats in the work and personal environments and includes, at a minimum, the importance of detecting potential insider threats by cleared Employees and how to report suspected activity to the insider threat program

designee. We provide briefings on methodologies used by adversaries to recruit trusted insiders and collect classified information, and particularly within information systems. We train on indicators of insider threat behavior and procedures to report such behavior, as well as to meet safeguards for protecting critical information and to fulfill security reporting requirements.

3.3. Annual Refresher Training

Our annual refresher training will be provided to all cleared Employees/Consultants to remind them of their obligation to protect classified information and provide any updates to security requirements and potential threats. Our annual refresher training reinforces the information provided during the initial security briefing, and it keeps cleared Employees informed of appropriate updates and changes in security regulations. Our Employees will complete an annual refresher training within thirty (30) days of receipt.

3.4. Debriefings

When a cleared Employee no longer requires a security clearance, access to classified information, or terminates employment with Purdue University, the Security Team will debrief them and remove them from access in the DCSA designated system of record (currently DISS). Our debriefs will be administered by the Security Team. The Employee will sign the debriefing acknowledgement section of the SF-312. For local individuals, the debrief shall be conducted in person whenever possible. For those not local or not available for an in person debriefing, the debriefing may be conducted via phone, email, or in some cases by mailing the SF-312 to the individual's home.

3.5. Consultants

Our cleared consultants will execute a consultant certificate that meets the NISPOM RULE requirements with Purdue University and follow all administrative Employee responsibilities. Our cleared consultants will not work on classified information at any location except the U.S. Government (USG) site.

3.6. Temporary Help Suppliers

A cleared temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, will be responsible for ensuring that required briefings (both initial and refresher training) are provided to their cleared personnel. The temporary help supplier or the using contractor may conduct these briefings.

3.7. Defense Counterintelligence and Security Agency

DCSA is the Government Cognizant Security Agency Office (CSA) which provides oversight of Contractors' procedures and practices for safeguarding classified defense information. Industrial Security Representatives (ISR) of DCSA may contact you in connection with the conduct of a Security Review (SR) or Continuous Monitoring (CM) of the facility, an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance to you and the Company on security related issues.

3.8. Security Review (SR) and Other DCSA Assessments

DCSA does not have a set schedule of when they are going to conduct an SR or CM review of the facility. During these assessments, DCSA ISR will review our security practices and procedures to ensure compliance with the NISPOM RULE and interview our Employees to assess the effectiveness of our security program. Your cooperation with DCSA during the SR/CM is required per the DOD Security Agreement form that was executed between Purdue University and the Government.

3.9. Contractor Review/Self-Inspections

Our Security Team will perform a Self-Inspection, similar to the DCSA Security Review/CM, at least once every twelve (12) months. The purpose of our Self-Inspection is to identify any vulnerabilities in our security program, determine the effectiveness, and identify any deficiencies/weaknesses in our practices and procedures. As part of

this process, our Security Team will interview Employees/Consultants. A formal report describing the Self-Inspection and its findings will be provided to DCSA for review. Our process will be based on the DCSA Self-Inspection Handbook, and a final report identifying each chapter will be prepared at the end. The Self-Inspection will be conducted by the Security Team and will be presented to all Key Management Personnel (KMP) and approved by the Senior Management Official (SMO).

Our Self-Inspection will be conducted at a minimum annually during the month of August. .

4. Individual Reporting Responsibilities (SEAD 3)

All Employees are to report to the Security Team any of the information within this Section. Send reports to FSO@purdue.edu.

4.1. Adverse Information

Adverse information is any information regarding a cleared Employee/Consultant, or an Employee/Consultant in process for a clearance, which suggests that their ability to safeguard classified information may be impaired, or that their access to classified information may not be in the best interest of National Security. Cleared personnel should report adverse information regarding themselves or another cleared individual to the Security Team. The Security Team will submit a finalized report to the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCSA CAS) via Defense Information System for Security (DISS) or the appropriate government system. Reportable adverse information includes, but is not limited to:

- Relationships with any known saboteur, spy, traitor, anarchist, or any espionage or secret agent of a foreign Nation
- Serious mental instability, or treatment at any mental institution
- Use of illegal substances, or excessive use of alcohol, or prescription drugs (to include Marijuana)
- Excessive debt, including garnishments of Employee's wages, and debt delinquent over 120 days
- Unexplained affluence/wealth
- Unexplained absence from work for periods of time that is unwarranted or peculiar
- Criminal convictions involving a gross misdemeanor, felony, or court martial
- Violations and deliberate disregard for established security regulations or procedures
- Unauthorized disclosure of classified information
- Members of, or individuals sympathetic to, an organization aiming to overthrow the U.S. Government by unconstitutional means
- Involvement in the theft of, or any damage to, Government property
- Misuse of Information Systems

Note: Reporting adverse information does not necessarily mean the termination of a personnel clearance. Reports should not be based on rumor or innuendo.

4.2. SEAD 3 Reporting Requirements

The FSO will provide the following baseline reports upon occurrence. See the complete SEAD 3 Directive located at the end of this SPP which contains the Appendices mentioned below with the required elements for reporting.

ACTIVITY CATEGORIES	CONTRACTOR GUIDANCE & CLARIFICATION FOR REPORTING BY ALL COVERED INDIVIDUALS (REMINDER: **"Covered Individuals"** refers only to those contractor personnel who have been granted eligibility for access	TYPES OF REPORTING REQUIRED BY CLEARED CONTRACTOR	REQUIRED DATA ELEMENTS FOR

	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.)	(FSO OR ASSIGNED DESIGNEE) IN DISS OR SUCCESSOR SYSTEM	SUBMITTED REPORTS
Psychological and Emotional Health	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.	Incident Customer Service Report entered	Provide applicable information.
Foreign Contacts - OFFICIAL	• Contact with foreign nationals occurring solely as part of a covered individual's official duties, and absent any bonds of affection or obligation, is **not required to be reported**. • 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, is **not required to be reported**. (See SEAD 3, D.8 and F.2.a)	N/A	N/A

	In cases of an official foreign contact deemed by the cleared contractor (FSO or assigned designee) to be a security concern, an incident report shall be submitted into DISS.	Incident Customer Service Report entered	See SEAD 3 Appendix A, 2. or 3.
Foreign Contacts -UNOFFICIAL	• Unofficial contact with a known or suspected **foreign intelligence entity**. In addition, the cleared contractor (FSO or assigned designee) should also report this activity directly to their DCSA Counterintelligence Special Agent (CISA). If you need assistance identifying or contacting your designated CISA please visit https://www.dcsa.mil/mc/ctp/locations/. • **Continuing association** with known foreign nationals that involves **bonds of affection**, **personal obligation, or intimate contact.** (See SEAD 3, D.8 and F.2.b.2)) A covered individual employed by a cleared contractor with foreign affiliations (e.g., FOCI, multinational business structure) only needs to report such continuing associations if they involve bonds of affection, personal obligation, or intimate contact.	Customer Service Report entered	See SEAD 3 Appendix A, 2.
	• Any contact with a foreign national involving the **exchange of personal information**. (See SEAD 3, D.8 and F.2.b.2)) • A reportable instance involving an exchange of personal information with a foreign national would meet the following criteria: 1. The name and nationality of the foreign national are known by the covered individual during or after the exchange of personal information, 2. 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 3. Contact with the foreign national is re-occurring or expected to re-occur.	Customer Service Report entered	See SEAD 3 Appendix A, 3.
	Updates regarding continuing association with known foreign nationals (See SEAD 3, D.8 and F.2.b.2))	Customer Service Report entered	See SEAD 3 Appendix A, 3.

Behavior & Conduct	See SEAD 3, F.3. for a list of actions or activities of covered individuals that are **reportable by other covered individuals** to the cleared contractor (FSO or assigned designee).	Incident Customer Service Report entered	See SEAD 3 Appendix A, as applicable
	Attempted **elicitation, exploitation, blackmail, coercion, or enticement** to obtain classified information or other information specifically prohibited by law from disclosure. (See SEAD 3, G.2.a)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 13.
Foreign Affiliation	Application for or receipt of **foreign citizenship**. (See SEAD 3, G.1.a and H.1.d.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 7.
	Application for, possession, or use of a **foreign passport or identity card** for travel. (See SEAD 3, G.1.b. and H.1.e.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 8. and 9.
	Voting in a **foreign election**. (See SEAD 3, H.1.f.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 11.
Media Contact	Contact with the media: • if the media seeks or shows interest in classified information or information otherwise prohibited from public disclosure, and; • if an associated investigation/ inquiry reveals a mishandling and/or unauthorized disclosure of classified information. (See SEAD 3, G.2.b. and H.2.b)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 14.
Criminal Activity	**Arrests.** (See SEAD 3, G.2.c. and H.2.c.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 15.
Treatment and Counseling	**Alcohol- and drug-related treatment**. (See SEAD 3, G.2.e., H.2.h.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 19.
Personal Finance & Business Interests	**Bankruptcy** or over 120 days delinquent on any **debt.** (See SEAD 3, G.2.d. and H.2.d.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 16.
	Financial Anomalies Examples include, but are not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain. (See SEAD 3, H.2.d.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 16.
	Direct involvement in **foreign business**. (See SEAD 3, H.1.a.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 4.

	Foreign **bank accounts**. (See SEAD 3, H.1.b.)	Incident Customer Service Report entered	See SEAD 3 Appendix A, 5.
	Cryptocurrency. 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.	Incident Customer Service Report entered	• Name of crypto- currency • Exchange host country • Dollar value of the asset
	Ownership of **foreign property**. (See SEAD 3, H.1.c.) Includes ownership interest in foreign real estate. For the purpose of ISL, this includes land, any inherently permanent improvements to land (e.g., buildings, living spaces), or ownership of rights associated with the land or the inherently permanent improvements to the land, to include right-to-use time share agreements and natural resource rights. Diversified investments (e.g., index funds.) do not need to be reported unless they are entirely composed of property holdings in a foreign country or countries.	Incident Customer Service Report entered	See SEAD 3 Appendix A, 6.
Living Status/ Arrangements	**Cohabitant**(s): 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). (See SEAD 3, D.3 and H.2.f.)	Customer Service Report entered	See SEAD 3 Appendix A, 17.
	Marriage: All civil marriages, legally recognized civil unions, and legally recognized domestic partnerships. (See SEAD 3, H.2.g.)	Customer Service Report entered	See SEAD 3 Appendix A, 18.
	Adoption of non-U.S. citizen children. (See SEAD 3, H.1.g.)	Customer Service Report entered	See SEAD 3 Appendix A, 12.
	Foreign National **Roommate(s)** (See SEAD 3, D.8 and H.2.e.)	Customer Service Report entered	See SEAD 3 Appendix A, 3.

Foreign Travel -UNOFFICIAL	• Unofficial foreign travel **is required to be reported at least 30 days in advance** (See SEAD 3, F.1.b for exceptions). • 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" as stipulated below at the end of this table.	Foreign Travel Module	Itinerary data: -Countries visited - Travel dates - Travel modes & carriers Passport data: - Full name - Issuing country - Passport # - Issuance date - Expiration See SEAD 3, Appendix A, 1: items e, f, h, and as needed g, i, and j.
	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. (See SEAD 3, F.1.b.1))	Foreign Travel Module	
	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. (See SEAD 3, F.1.b.1)b))	Foreign Travel Module	
	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. (See SEAD 3, F.1.b.1)d))	Foreign Travel Module	
	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.	Foreign Travel Module	
	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.	Foreign Travel Module	
Foreign Travel – UNOFFICIAL (Related Cleared Contractor Actions)	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;	Foreign Travel Module	Itinerary data: - Countries visited - Travel dates - Travel modes & carriers Passport data: - Full name - Issuing country

	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 (See columns titled "Required Reporting By Cleared Contractor" and "Required Data Elements" for requested itinerary data.); 3. The cleared contractor provides the covered individual with the NCSC "Safe Travels" resource link for required review. 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 Additionally, the cleared contractor (FSO or assigned designee) must follow the following further guidance: 1.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, available here, then cleared contractor should provide information from this advisory to the covered individual. 2.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. 3. 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 link at least annually for required review. 4.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. (See SEAD 3, E. and F.)		- Passport # - Issuance date - Expiration See SEAD 3, Appendix A, 1: items e, f, h, and as needed g, i, and j.
Foreign Travel -OFFICIAL	• Official foreign travel **is not required to be reported**. • 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. (See SEAD 3, F.1.a.)	N/A	N/A

SEAD 3 entrusts all covered individuals with the critical responsibility to report behavior or activities of those around them that could compromise classified information, workplace safety, and/or our National Security.

4.3. Espionage/Sabotage

Report any information concerning existing or threatened espionage, sabotage, or subversive activities. The FSO will forward a report to the Federal Bureau of Investigation (FBI) and DCSA.

4.4. Suspicious Contacts

Suspicious contacts are efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified or unclassified United States Government information or to compromise cleared Employees. Personnel should report all suspicious contacts to the Security Team. The FSO forwards all reports to the respective government agency for review and action.

4.5. Citizenship by Naturalization

Contractors will report if a non-U.S. citizen Employee granted an LAA becomes a citizen through naturalization. The report will include: (i) City, County, and State where naturalized, (ii) Date naturalized, (iii) Court, And (iv) Certificate number.

4.6. Classified Information Non-Disclosure Agreement (SF-312)

Contractors will report instances when an Employee no longer wishes to be processed for a determination of eligibility for access to classified information or to continue having access to classified information and the reason for that request.

Purdue University will report the refusal by an Employee to sign the SF-312, "Classified Information Nondisclosure Agreement," or other approved NDA. These incidents will be submitted via DISS.

4.7. Loss, Compromise, or Suspected Compromise of Classified Information

Cleared personnel must immediately report the loss, compromise, or suspected compromise of classified information to the Security Team. In turn, the FSO will immediately notify DCSA and request further guidance and assistance.

Should a piece of electronic equipment be compromised, regardless of classification level and/or ownership, DCSA has the right to take ownership of such property. An example is an individual's personal cell phone with email capability that received a classified email by mistake.

4.8. Data Spills

Spillage, also referred to as a data spill, is a security incident that results in the transfer of classified information onto an information system not authorized to store or process that information In the event of a data spill, the Employee is expected to:

- Immediately report the data spill
- Do not delete or forward the classified data to anyone else (including security personnel)
- Isolate the system to minimize damage and preserve evidence
- Use caution when discussing the incident over the phone
- Consider that the location and nature of the spill may be classified

Once a data spill is reported, the appropriate personnel will assess possible risks as a result of contamination and follow any special guidelines provided by the data owner. Once the extent of the spillage is determined and the exact location of information systems is known, the Activity Security Manager or FSO will immediately coordinate with the data owner and plan the investigation/cleanup. This will include detailed information such as sender and recipient(s), subject, date and time, and the potentially affected systems. If the security inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the Activity Security Manager or

FSO will submit an initial report via secured channels to the DCSA IS Rep along with any other agencies that may need to be notified.

Once the risk assessment is complete, those in charge of the data spill will assign or work with appropriately cleared personnel during the cleanup effort. Specific cleanup procedures will include:

Prior to sanitization:

- Ensure approved procedures are on file and data owner approves
- Conduct a cost analysis to determine if destruction is more cost effective

Sanitization:

- Use NSA- and NIAP-authorized procedures and products
- Tag all sanitized hard drives

FSO:

- Get written statements from all personnel involved in actual incident and the resulting cleanup
- Submit final report to DCSA
- Coordinate storage and transfer of classified material and evidence

4.9. Security Violations

Cleared personnel must report any failure to comply with a requirement of this SPP, or of the NISPOM RULE, to the Security Team.

4.10 Security Equipment Vulnerabilities

All personnel must report significant vulnerabilities in security equipment or hardware/software that could possibly lead to the loss or compromise of classified information to the Security Team.

4.11 Reinvestigations and Continuous Evaluation

Continuous evaluation (CE) is a personnel security investigative process and is part of the security clearance reform effort to modernize personnel security processes and increase the timeliness of information reviewed between periodic reinvestigation cycles. CE supplements and enhances, but does not replace, established personnel security processes. CE is a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual's continued eligibility. Our Security Team will validate that the Employee requires continued eligibility for access to classified information before initiating the reinvestigation.

5. Graduated Scale of Disciplinary Actions

Purdue University has an established system to manage and track information regarding Employees with eligibility for access to classified information who violate the requirements of this rule in order to identify patterns of negligence or carelessness, or to identify a potential insider threat.

Purdue University has established and will enforce policies that provide appropriate administrative actions taken against Employees who violate requirements of the NISPOM RULE. We have established and applied a graduated scale of disciplinary actions in the event our Employees are involved in violations or negligence. A statement of the administrative actions taken against an Employee will be included in a report to DCSA when individual responsibility for a security violation can be determined, and one (1) or more of the following factors are evident:

a) The violation involved a deliberate disregard of security requirements.
b) The violation involved gross negligence in the handling of classified material.
c) The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness.

All Individual Culpability Reports shall be brought to the attention of the FSO immediately. An investigation shall be conducted by the FSO, and all reports shall be submitted to the DCSA ISR. At a minimum, the DCSA ISR shall be notified of all pending reports as soon as the FSO is made aware, and a record of all reports shall be archived in the information management system.

Purdue University has established a graduated scale of administrative sanctions, up to and including dismissal from employment. As a general rule, security may recommend an appropriate sanction(s); however, Senior Management will make the final determination of the sanction(s) to be administered.

Several factors determine the administrative or disciplinary actions to be applied to persons found responsible for a security incident or violation, including: severity of the incident; extenuating circumstances; history of previous security-related incidents or violations; willful disregard for security procedures; and loss or compromise of classified information or materials.

Employees who violate these procedures are subject to disciplinary action. Disciplinary action may include, but is not limited to, the following or a combination thereof:

- Remedial training;
- Verbal warning - notification and warning to employee (may or may not be documented in writing);
- Written reprimand - formal notification in writing to employee; this may take the form of a “last chance” letter to inform the employee that termination will result should another violation occur;
- Suspension - loss of work and wages for a number of days, as determined by the University. Note that all employees may be subject to an unpaid disciplinary suspension (whether for a full day or a longer increment as determined by the University), regardless of their exempt or non-exempt status. Note that, for non-exempt employees, a suspension may be based on partial-day increments; and
- Loss of security clearance
- Discharge - termination of employment.

A graduated scale of disciplinary action requires a consistent increase in the corrective measures taken against an individual who has violated security procedures on more than one occasion. The disciplinary action to be taken for a specific violation will be based on a variety of factors, including, but not limited to, the nature and severity of the violation, nature and severity of previous infractions, frequency of violations, intent (negligent, willful, planned), and any relevant external factors. Multiple violations within a one-year period indicate a pattern of non-compliance with security procedures.

Additional corrective measures may include the following:

- Removal from a specific research program
- Suspension of access to classified information
- Termination of security clearance
- Criminal action

Our SMO reserves the right to implement the most stringent administrative sanctions up to and including termination if they deem the incident is severe enough to warrant. Further, should management identify that the individual is a serious threat to National Security, they without authority from any other KMP in the Company or Shareholders’ approval may terminate the individual access to classified materials at any time pending review by the Company and DCSA.

6. Physical Security

6.1. Storage (NISPOM Reference 117.15C2)

Our Facility is authorized to store classified material; therefore, we are required to establish a system of security checks at the close of each working day to ensure that all classified material has been appropriately secured. This means that all security containers (i.e. safes) used for the storage of classified material require a hands-on check at the end of each working day. The check should include spinning the dial of the container a minimum of four times in either direction and checking each drawer handle; a visual check of the area around the container; and, if appropriate, any other area classified material is worked on (i.e., conference room, computer room, etc.). Our safes will have a Security Container Check Sheet (SF 702). Open Storage Areas and Secure Areas will have an Activity Security Checklist (SF 701) and a Security Container Check Sheet (SF 702). Secure Area means all items computers, documents, media etc. are required to be locked in a GSA (Government Services Administration) approved container at the end of use.

6.1.a Safe

Our GSA approved container shall be accompanied with a Security Container Check Sheet (SF 702) and an Access Roster. Our GSA approved containers shall be locked when not in use.

6.1.b Combinations to Lock

Our FSO is the only authorized employee to change the combination under any of the following conditions: (1) a newly acquired safe; (2) an employee knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or (3) whenever a combination has been the subject of possible unauthorized disclosure.

6.1.c Classified Meetings

Utilization of conference or meeting rooms for classified meetings may occur if a determination is made that controls can preclude unauthorized access to classified information.

In all instances of classified meetings, the FSO or their designee will:

1. Determine that the visit is necessary, and the purpose of the visit cannot be achieved without access to, or disclosure of, classified information.
2. Ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information.
    a. The responsibility for determining the need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. The need-to-know is generally based on a contractual relationship between the contractors. In other circumstances, disclosure of the information will be based on an assessment that the receiving contractor has a bona fide need to access the information in furtherance of a GCA purpose.
    b. Verification of a visitor's PCL may be accomplished by a review of a CSA-designated database that contains the information or by a visit authorization letter (VAL) provided by the visitor's employer.
        i. If a CSA-designated database is not available and a VAL is required, contractors will include the following in all VALs:
            1. Contractor's name, employee's name, address, and telephone number assigned commercial and government entity (CAGE) code if applicable, and certification of the level of the entity eligibility determination.
            2. Name, date and place of birth, and citizenship of the employee intending to visit.

3. Certification of the proposed visitor's PCL and any special access authorizations required for the visit.
4. Name of person(s) to be visited.
5. Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit.
6. Date or period during which the VAL is to be valid.

3. Ensure visitors are only afforded access to classified information consistent with the purpose of the visit.
4. Ensure visitors do not bring personal electronic devices into the meeting space.

6.1.d Classified Work Areas

Classified work will only be conducted in areas accredited at the appropriate level. Exceptions to this rule will be reviewed on a case-by-case basis by the FSO, AFSO, ISSM, and/or Security Operations Manager.

6.1.e In-Use Controls

Each Employee must ensure that classified material in their custody is not subjected to access by unauthorized persons. In-use controls refer to the procedures utilized to ensure that classified material is handled in a manner that precludes unauthorized access.

Each classified document shall have a coversheet (SF 703, SF 704, or SF 705). These coversheets shall also contain the document control number associated with the document. This number shall be generated from the FSO. Coversheets shall be attached to the front and back of every classified document.

In-Use Controls are meant to preclude visual access for any other party that may be in the same area as you when utilizing classified information. When in use, doors shall be locked, blinds shall be closed, and any other possible actions shall be taken to preclude visual or verbal access.

If a visitor requires access to an area above their clearance level, the visitor's escort will announce their presence, turn on the blue visitor light (if available), and allow the visitor to enter only after all material above the visitor's clearance and access level has been stored. Information outside of the visitor's need-to-know will also be stored, even if the visitor has the appropriate clearance.

6.1.f Visitor Control (Individual Spaces)

Visitor control shall be implemented for every location, permanent or temporary, where classified information is being utilized. While in process you should be able to control the visitors entering your space. This can be done by locking doors and following the In-Use Control procedures.

7. Control and Accountability of Classified Information

7.1. Information Management System

Our Facility is required to establish an Information Management System (IMS)., For circumstances involving IMS, control means to properly handle and safeguard all classified material; received, generated, reproduced, and destroyed. The IMS established should be clearly recognizable and consistent.

7.2. Transmission of Classified Information by Mail (NISPOM Reference 117.15F)

This section governs when Purdue University receives classified mail or is sending classified mail. Only the FSO or their designee shall receive and/or send classified mail.

Classified information shall be transmitted and received in an authorized manner to ensure that evidence of tampering can be detected inadvertent access can be precluded, and delivery to the intended recipient is timely.

Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with 32 CFR 2001.

7.2.a. Receipt of Classified Information by Mail

When Purdue University is receiving classified mail, the individual responsible for the mail at the Company shall be cleared to the level of safeguarding and shall immediately bring the classified mail to the FSO or their designee immediately upon receipt. At no time shall classified mail be left unattended or handled by an uncleared individual.

In some cases, we may use a Post Office Box for classified mail. In these cases, the FSO shall control access to and regularly check the P.O. Box.

Further, the classified mailing address shall be listed in National Industrial Security System (NISS).

This classified information will be required to have a new control number, coversheets placed on the document, a custodian assigned to the information, a contract assigned to the information, and a specific safe in which the information is to be secured is assigned.

7.2.b. Transmitting Classified Information by Mail

The FSO or their designee shall be the only individuals who are authorized to transmit classified materials. When doing so, a receipt and dispatch record shall be generated from the FSO and shall accompany the information being transmitted. The receiver of the information shall return a signed transmittal certificate upon receipt and a copy of the signed transmittal certificate shall be sent to the FSO for retention. At no time shall the receipt/transmittal certificate contain any classified information. When transmitting by mail, it is imperative to refer to 32 CFR 2001.46 for proper transmission of classified information. A copy of the 32 CFR 2001.46 can be found on ecfr.gov.

7.2.c. How to Package Classified Information

The FSO or their designee shall be the only individuals that are authorized to package classified information for transmission. When transmitting by mail, it is imperative to comply with NISPOM RULE for proper packaging and addressing of classified packages. A copy of the NISPOM RULE can be found at ecfr.gov.

Classified material must be packaged in a way that minimizes the risk of accidental exposure and facilitates the detection of deliberate tampering. Classified materials will be packaged appropriately for the content and size of the item, such as envelopes and small parcels, briefcases and pouches, and large bulky items. In addition to the NISPOM RULE, classified information must be transmitted in accordance with DoDM 5200.01, Volume 3, Enclosure 4, “DoD Information Security Program”.

7.3. Utilization of Couriers (NISPOM Reference 117.15F4)

Courier means a cleared employee, designated by the FSO, authorized to hand-carry classified material to its destination, ensuring that the classified material remains under their constant and continuous protection and that they make direct point-to-point delivery.

7.3.a. Receipt of Classified Information by a Courier

Should any courier, internal or external to Purdue University, introduce classified materials into our Facility, the classified information shall be brought immediately to the FSO or their designee. This classified information is required to have a new control number issued from the FSO, coversheets placed on the document, a custodian assigned to the information, a contract assigned to the information, and assigned a specific safe in which the information is to be secured.

7.3.b. Transmitting by Courier

Only our FSO or their designee shall approve couriers. Individuals approved as couriers shall complete a courier briefing and retain a courier badge or letter authorizing them to be a courier. Couriers shall be trained to courier classified materials and shall be given specific instructions at the time of dispatch of proper handling for that specific package.

The FSO or their designee must do all of the following:

1. Brief employees providing courier services on their responsibility to safeguard classified information and keep classified material in their possession at all times.
2. Provide employees with an identification card or badge which contains the contractor's name and the name and a photograph of the employee.
3. Make arrangements in advance of departure for overnight storage at a USG installation or at a cleared contractor's facility that has appropriate storage capability, if needed.
4. Conduct an inventory of the material prior to departure and upon return. The employee will carry a copy of the inventory with them.

7.4. Destruction of Classified Information (NISPOM Reference 117.15G1/2)

Destruction of classified information shall only be done by the FSO or their designee. Our Facility will destroy classified material in accordance with 32 CFR 2001.47 with equipment that is compliant with 32 CFR 2001.42(b). If our facility does not have the equipment to properly destroy a medium of classified material, it will be transferred to an authorized Facility in accordance with transmission procedures.

If we destroy classified information, a destruction certificate shall be generated by the FSO for the information destroyed and the parties who destroyed the information shall sign the destruction certificate. The signed destruction certificate will be retained by the FSO.

7.4.a. Standards for Security Equipment (NISPOM Reference 117.15B)

Purdue University follows guidelines established in the NISPOM RULE, when procuring storage and destruction equipment. Authorized repairs for GSA-approved security containers and vaults must be in accordance with Federal Standard 809. Our Facility will comply with the destruction equipment standard stated in § 2001.42(b) of 32 CFR 2001.

7.5. Disclosure (NISPOM Reference 117.15H)

Purdue University has established a process by which classified information is disclosed only to authorized persons with the appropriate eligibility for access to classified information and need-to-know for the performance of tasks or services essential to the fulfillment of a classified contract or subcontract. Purdue University will not disclose classified information to the public.

7.5.a. Disposition (NISPOM Reference 117.15I)

The FSO or Employee designee will review all classified holdings annually to ensure that the information is in support of a current contract.

7.5.b. Retention (NISPOM Reference 117.15J)

The provisions of §117.13(d)(5) apply for retention of classified material upon completion of a classified contract. Purdue University shall promptly return all classified information to USG.

7.5.c. Termination of Security Agreement (NISPOM Reference 117.15K)

If the CSA terminates the Facility's eligibility for access to classified information, Purdue University shall return all classified material in its possession to the GCA.

8. Visitor Control (Building)

8.1. Perimeter Controls (NISPOM Reference 117.15A3)

Pursuant to 32 CFR Part 117.15 (a)(3), our Facility has established a perimeter control system to deter and detect unauthorized introduction of classified material into or removal of classified material from the Facility.

The variety of sizes, locations, and security programs at our facility present some unique situations necessitating a flexible policy. However, to follow and implement this procedure, the FSO or designated person at each entrance/exit shall conduct random inspections. These inspections will be limited to that which is necessary to determine whether classified information is contained in briefcases, handbags, backpacks, luggage, packages, etc. Inspections are not required of wallets, change purses, clothing, cosmetic cases, or other objects of an unusually personal nature.

In connection with this requirement, each Facility must also post signs at entrances/exits informing persons who enter or leave the Facility that they are subject to an inspection of their personal effects. The sign shall read "Warning – Restricted Area – Keep Out – Authorized Personnel Only – Authorize entry into this restricted area constitutes consent to search of personnel and the property under their control – Internal Security Act of 1950 – Section 21: 50 U.S.C. 797"

All visitors in the Facility shall have restricted access and shall be always escorted within the Facility by a cleared escort.

8.2. Logbook and Access by Visitors

Our Facility has implemented a Visitor Logbook. The Visitor Logbook shall, at a minimum, include the visitor's name, entity the visitor is representing, citizenship status, classified visit (Yes/N

If any visitor indicates on the Visitor Logbook that they are a Non-U.S. Person, the FSO shall be immediately notified and shall approve or disapprove the visitor access to the Facility.

Additionally, if the visitor indicates they are present for a classified Visit, the FSO shall verify in Defense Information System for Security (DISS) that a visit request exists, and the person has the appropriate level of clearance for the purpose of their visit.

8.3. End of Day Security Checks (NISPOM Reference 117.15A2)

This is performed by the FSO or an appointed cleared person to ensure all information and storage containers have been properly secured. If the cleared Employees are working at the government location or offsite, they will follow the appropriate Facility requirements of that cleared location.

9. Defense Hotline

The Department of Defense (DoD) provides a Defense Hotline as a confidential avenue for individuals to report allegations of wrongdoing pertaining to programs, personnel, and operations that fall under the purview of the DoD, pursuant to the Inspector General Act of 1978. Anyone, including members of the public, DoD Personnel, and DoD Contractor Employees may file a complaint with the DoD Hotline.

The Defense Hotline number is below.

DEFENSE HOTLINE
THE PENTAGON
WASHINGTON, DC 20301-1900
TELEPHONE: 800-424-9098
http://www.dodig.mil/hotline

10. Marking Classified Information

10.1. Classification Levels

- **TOP SECRET** - Material that if compromised could cause "Exceptionally Grave Damage" to National Security and requires the highest degree of protection.
- **SECRET** - Material that if compromised could cause "Serious Damage" to National Security and requires a substantial degree of protection.
- **CONFIDENTIAL** - Material that if compromised could cause "Damage" to National Security.

10.2. Original Classification

The determination to originally classify information may be made ONLY by a United States Government official who has been delegated the authority in writing. Information is classified pursuant to Executive Order 13526 and is designated and marked as Top Secret, Secret, or Confidential. Contractors make derivative classification decisions based on the guidance provided by the Contract Security Classification Specification (DD Form 254) and Security Classification Guidance applicable to each classified contract.

10.3. Derivative Classification

Derivative classification is the reproduction, extraction, incorporation, or paraphrasing of already classified information into a new form. This may ONLY be done by Employees specifically authorized to perform derivative classification actions who have completed the required training.

Employees who have been authorized to make derivative classification decisions must complete initial derivative classification training and a refresher training at least once every two (2) years, prior to being authorized to make derivative classification decisions. Documentation will be retained identifying the date of the most recent training and the type of training received: initial or refresher. Contact the Security Team for guidance on how to access and complete the training. Our Employees are not authorized to conduct derivative classification before completing such training. Duplication or reproduction (i.e., copying, or printing existing documents, forwarding classified emails, etc.) is NOT derivative classification.

10.4. Controlled Unclassified Information (CUI) Markings

CUI is government created or owned unclassified information that must be safeguarded from unauthorized disclosure. CUI policy provides a uniform marking system across the Federal Government that replaces a variety of agency-specific markings such as FOUO, LES, SBU, etc. The implementation of the DoD CUI Program addresses the designation, handling, and decontrolling of CUI in accordance with DoDI 5200.48. This includes CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management. Unclassified information can only be characterized as CUI if there is a law, regulation, or government-wide policy prescribing safeguarding or dissemination control. Agencies must not cite the Freedom of Information Act (FOIA) as a CUI safeguarding or disseminating control authority for CUI. While outside the requirements of the NISPOM RULE, when a classified contract includes provisions for CUI training, contractors will comply with those contract requirements. Government and Industry partners should notify the DCSA CUI Program Office mailbox at dcsa.quantico.ctp.mbx.esocui@mail.mil of any instances involving unauthorized disclosure of, or threats to, CUI.

11. Classified Discussions

Employees will ensure that classified discussions will not take place over unsecure telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons. If you need to have a classified discussion, contact the Security Team to determine which areas have been designated for classified discussions. Classified oral discussions shall only be done at cleared sites.

12. Public Release/Disclosure

Purdue University is not permitted to disclose classified or unclassified information pertaining to a classified contract to the public without prior review and approval by the Government Customer. If you have a need to perform a presentation, or create brochures, promotional sales literature, reports to stockholders, or similar materials on subject matter related to a classified contract, even if unclassified, please contact the Security Team to determine if we must obtain approval from the Customer.

Note: Classified information made public is not automatically considered Unclassified. Employees will continue the classification until formally advised to the contrary.

13. New Hire and On-boarding Process

The following procedures are in addition to the Human Resources (HR) Policy.

13.1. Initial Onboarding Responsibilities

Upon receipt of a signed acceptance of an offer letter for a new Employee who requires a security clearance, HR will notify the FSO. The FSO will identify the specific contract(s) the Employee is supporting, the highest level of security access required, and what, if any, classified computer system access is required.

13.2. Initial Security Team Responsibilities

All new hires who have a need-to-know and an existing or pending personnel security clearance and are supporting a contract with an active DD Form 254 will be owned in the designated system of record for personnel security clearances.

During the onboarding, the Security Team will send the new hire the following documents, including but not limited to:

- SF-312
- Initial Security Briefing
- SPP
- Type A Consultant Certificate (if the new hire is a 1099 Independent Consultant)

All new hires who do not have a personnel security clearance and require a new SF-86 for eligibility will:

- Provide proof of United States Citizenship (U.S. Passport, Birth Certificate, Naturalization Certificate, etc.)
- Complete an SF-86 via Electronic Questionnaires for Investigation Process (e-QIP)
- Complete fingerprinting and submit via SWFT to OPM (valid for 120 days)

When entering a new hire in the designated system of record for personnel security clearances, the following actions shall be taken, after the receipt of all documentation:

- The Company will validate and ensure the individual is being placed under the correct Commercial and Government Entity (CAGE) Code.
- The Security POC will identify the new hire’s category based on the following:

    - If the individual is a Form W-2 Employee, the individual will be categorized as a "Contractor".
    - If the individual is a Form 1099 Independent Consultant, the individual will be categorized as a "Consultant".
    - DCSA will advise the Security Team how to list subcontractors if the GCA requires them to be in the Subject Listing under the prime contract and on a Joint Visit Request.
- Security Team will take an "owning" or "servicing" relationship, depending on the new hire's status.
- Security Team will insert an "In Processing Date".
- Security Team will insert the appropriate access level, as determined by the FSO and Manager.

14. Change in Employee Status

The FSO or the Employee will report any of the following Employee status changes:

- Change in Name
    - A name change will require supporting documentation. The Security Team shall modify in DISS/NBIS the new name and provide supporting documentation to the Vetting Risk Operations (VRO).
- Change in Employment Status (New Hire, Separating, Leave of Absence (LoA), Leave without Pay (LWOP)):
    - For Employees separating from Purdue, the Security Team will have the employee sign the debriefing portion of the SF312, remove the employee's access in DISS, and unown the subject in personnel security system of record.
    - Any Employee on LoA or LWOP, shall have their access in DISS/NBIS removed pending the resolution of status.
- Change in Contract
    - The Security Team shall revalidate their requirement for access to classified materials, the level of access required, the continuous needs of access to Government systems. If any requirements change, the accesses shall be modified to satisfy the current requirements.
- Change in Job Position/Title
    - The Security Team shall revalidate their requirement for access to classified materials, the level of access required, the continuous needs of access to Government systems. If any requirements change, the accesses shall be modified to satisfy the current requirements.

15. Security Access Validations

Access levels in DISS/NBIS will be reviewed and validated on an ongoing basis. The Security Team will meet with the Controller, HR, Program Manager, or other appropriate individuals to review the current list of Employees and/or Consultants to compare the DISS subject report to the payroll report and with the current access requirements the Program Manager provides for that period.

The Employee's Program Manager shall be able to provide the contract number and highest level of classification required for each individual who is under the CAGE code.

The Security Team will modify any access, as required, based on these meetings.

16. Separations and Terminations

The direct supervisor shall immediately notify Human Resources upon any termination or resignation HR shall notify the FSO if the employee's clearance was owned by Purdue University.

The Security Team will reach out to the Employee to begin out-processing.

The Security Team will ensure the following actions occur:

- In DISS/NBIS, the indoctrination level is removed, an out-processing date is entered, and a separation date is entered with the appropriate category. ** At no time shall the out-processing date or separation date be back- or post-dated without express authority of DCSA and/or a Federal Judge.
    - "Separation" will be used for any Employee that terminates.
    - "Deceased" will be used for any Employee who has passed away.
    - "Invalid Entry" will be used for any contingent hire or new hire where the individual did not actually physically start with the Company.
    - "Facility Termination" will only be used by the Government upon the Facility Clearance being inactivated.
- The Employee will complete the debriefing section of the SF-312 or similar form. If the employee is not available to do an in-person debrief, the FSO will conduct an "Admin Debrief".
- The Employee will certify that he/she has returned all equipment and proprietary information (as applicable).
- The Employee's physical access to the building shall be inactivated and/or removed.
- The Security Team will remove any NISS/DISS/NBIS Accounts associated with the Employee, if applicable.

17. Visit Procedures

17.1. Incoming Visits

All incoming classified visits must be approved in advance by the Security Team. The Security Team will verify each visitor's security clearance prior to allowing classified access. The Security Team is responsible for determining that the requesting Contractor has been granted an appropriate FCL based on an existing contractual relationship involving classified information of the same or higher classification category, or otherwise by verification through the NISS. The Security Team will validate the individual's access level and appropriate visit request in DISS, prior to approving any visitor.

The responsibility for determining need-to-know in connection with a classified visit rests with the individual disclosing classified information during the visit. Prior to the disclosure of classified information to a visitor, proof of identification of the person must be accomplished.

17.2. Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When it becomes necessary for Employees to visit other cleared Contractors or Government agencies, and access to classified information is anticipated, Employees must notify the FSO and provide: the Contractor or agency to be visited, the time and duration of visit, the reason for the visit, and the person to be contacted. Allow at least one week for the visit request to be prepared, submitted via DISS to the Contractor/agency, and processed by their visitor control.

18. Initiating an Investigation in NBIS

All requested investigations and upgrades must be approved in advance of initiating the Electronic Application (eApp) by the FSO. The FSO will verify the Employee requires access in accordance with the NISPOM.

19. Special and Caveated Access/Information Systems

The FSO will verify all requested Special and Caveated accesses (i.e., Restricted Data (RD), Formerly Restricted Data (FRD), DoD Critical Nuclear Weapon Design Information (CNWDI), North Atlantic Treaty Organization (NATO), and Communications Security (COMSEC)) prior to being granted access. The FSO will be initially briefed by an Industrial Security Representative of DCSA before briefing any Employee.

Once the FSO is briefed by the ISR, the Employees may be briefed. Initial briefings and refresher briefings will be maintained in the Information Management System as needed.

National intelligence is under the jurisdiction and control of the Director of National Intelligence (DNI), who establishes security policy for the protection of national intelligence and intelligence sources, methods, and activities. In addition to the guidance in this Manual, Employees shall follow Intelligence Community Directives (ICDs), policy guidance, standards, and specifications for the protection of classified national intelligence and SCI.

19.1. Information Systems Security

All information system authorized users will receive training on the security risks associated with their user activities and responsibilities under the NISP. Purdue University will determine the appropriate content of the training, taking into consideration assigned roles and responsibilities, specific security requirements, and the information system to which personnel are authorized access.

Each classified information system is different. Should any of our systems be approved for classified processing there will be an Information Systems Security Manager (ISSM) appointed who works with the FSO to ensure NISP compliance.

Each information system shall be accompanied by a System Security Plan (SSP). Each individual requiring access to the information system shall have the appropriate clearance and received an Information Systems briefing. The briefing shall be maintained in the SSP book.

20. Emergency Procedures

20.1. Emergency Plan

In emergency situations, it is important to safeguard all classified information to the fullest extent possible. However, the overriding consideration in any emergency is the safety of personnel. Do not risk your life or the lives of others to secure classified information. For example, in case of fire, you may need to immediately exit the facility with the classified materials in your possession. Seek out the FSO for further instructions once in a safe environment.

20.2. Emergency Contact Numbers

The Emergency POC are the same as our Security POC. You will be notified via email if there is a change to the emergency contact list.

20.3. Government Site Emergency Procedures

Personnel working at Government sites should familiarize themselves with any local emergency procedures in place at that site.

21. Security Team

21.1. Operations

The Security Team can consist of both internal and external Security Officers supporting our program.

Internally we will maintain at a minimum the following positions:

- Senior Management Official (SMO)
- Facility Security Officer (FSO)
- Insider Threat Program Senior Official (ITPSO)
- Information Systems Security Manager (ISSM)

External individuals supplementing our internal team can consist of:

- Assistant Facility Security Officer (AFSO)
- Security Specialist (SS)
- Other Security Consultants as needed (i.e., Policy, IT Security Support, etc.)

The FSO will be responsible for directing all actions required by the Company. The support staff will prepare all paperwork for review and approval by the FSO as well as taking all actions as required in DISS/NISS.

21.2. Security Team Job Functions

Below are the job specific functions of each role.

Senior Management Official (SMO):

Ensure the contractor maintains a system of security controls in accordance with the requirements of this rule. Appoint a contractor Employee(s), in writing, as the FSO and appoint the same Employee or a different Employee as the ITPSO.

Insider Threat Program Senior Official (ITPSO):

The ITPSO will establish and execute an insider threat program.

- The ITPSO will be the main individual responsible for investigating, mitigating, and reporting all insider threats. These investigations will be done with the support of all security personnel as deemed necessary by the ITPSO. All reports the ITPSO receives will be reported to an Insider Threat Working Group for further examination.

Facility Security Officer (FSO):

Supervise and direct security measures necessary for implementing the applicable requirements of this rule and the related USG security requirements to ensure the protection of classified information

- The FSO will provide all leadership and direction on behalf of the Company for the security program. They will be the main interface between noncompliant individuals or individuals not completing their security requirements in a timely manner. This individual will also be the main POC who will interact with Government Customers.

Information Systems Security Manager (ISSM):

An ISSM will be appointed if there are Contractors who are, or will be, processing classified information on an information system located at our facility. The ISSM must be eligible for access to classified information to the highest level of the information processed on the system(s) under their responsibility. Our SMO will ensure that the ISSM is adequately trained and possesses technical competence commensurate with the complexity of classified information system. The FSO will notify the applicable CSA if there is a change in the ISSM. The ISSM will oversee development, implementation, and evaluation of our classified information system program. ISSM responsibilities are in 32 CFR117.18.

22. Definitions

The following definitions are common security related terms.

Access	The ability and opportunity to obtain knowledge of classified information.
Adverse Information	Any information that adversely reflects on the integrity or character of a cleared Employee, which suggests that his or her ability to safeguard classified information may be impaired or that his or her access

	to classified information clearly may be in the interest of National Security, or that the individual constitutes an insider threat.
Authorized Person	Authorized person means a person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know.
Classified Contract	Classified contract means any contract, license, agreement, or grant requiring access to classified information by a contractor and its Employees for performance. A contract is referred to in this rule as a "classified contract" even when the contract document and the contract provisions are not classified. The requirements prescribed for a "classified contract" also are applicable to all phases of precontract, license or grant activity, including solicitations (bids, 32 CFR Part 117: National Industrial Security Program Operating Manual (NISPOM RULE) page 6 of 96 quotations, and proposals), precontract negotiations, post-contract activity, or other government contracting activity (GCA) programs or projects which require access to classified information by a contractor.
Classified Information	Official Government information which has been determined to require protection against unauthorized disclosure in the interest of National Security.
Cleared Employees	All Employees granted a personnel clearance or who are in process for a personnel clearance.
Closed Area AKA 'Open Storage'	An area that meets the requirements outlined in the NISPOM RULE for safeguarding classified information that, because of its size, nature, and operational necessity, cannot be adequately protected by the normal safeguards, or stored during nonworking hours in approved containers.
Communications Security (COMSEC)	COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to National Security and to ensure the authenticity of such communications.
Compromise	An unauthorized disclosure of classified information.
CONFIDENTIAL	Classified information or material that requires protection whereby unauthorized disclosure could reasonably be expected to cause damage to our National Security.
Controlled Unclassified Information (CUI)	Government created or owned unclassified information that must be safeguarded from unauthorized disclosure.
Facility (Security) Clearance	An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).
Foreign Interest	Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.
Foreign National	Any person who is not a citizen or national of the United States.
Need-to-Know (NTK)	A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services to fulfill a classified contract or program.
Personnel Security Clearance (PCL)	An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.
Public Disclosure	The passing of information and/or material pertaining to a classified contract to the public or any member of the public by any means of communication.
SECRET	Classified information or material that requires a substantial degree of protection, the unauthorized disclosure of which could reasonably be expected to cause serious damage to our National Security.
Security Violation	Failure to comply with policy and procedures established by the NISPOM RULE that could reasonably result in the loss or compromise of classified information.
Standard Practices & Procedures (SPP)	A document prepared by contractors outlining the applicable requirements of the NISPOM RULE for the contractor's operations and involvement with classified information at the contractor's facility.
Subcontractor	A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.
TOP SECRET	Classified information or material that requires the highest degree of protection, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to our National Security.
Unauthorized Person	A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM RULE.

23. Abbreviations & Acronyms

AFSO	Assistant Facility Security Officer
AIS	Accredited Information System
C	CONFIDENTIAL
CAGE	Commercial and Government Entity
CNWDI	Critical Nuclear Weapons Design Information
COMSEC	Communications Security
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency (Formerly DSS)
DCSA CAS	DCSA Consolidated Adjudication Services (Replaced DOD CAF)
DISS	Defense Information System for Security
DoD	Department of Defense
DOE	Department of Energy
DTIC	Defense Technical Information Center
eApp	Electronic Application (Replaced e-QIP)
FBI	Federal Bureau of Investigations
FCL	Facility (Security) Clearance
FCV	Facility Clearance Verification
FGI	Foreign Government Information
FOCI	Foreign Ownership, Control, or Influence
FRD	Formerly Restricted Data
FSO	Facility Security Officer
GCA	Government Contracting Activity
GSA	General Services Administration
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITAR	International Traffic in Arms
ITPSO	Insider Threat Program Senior Official
KMP	Key Management Personnel
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Program Operating Manual
NISPOM RULE	CFR 32 Part 117 National Industrial Security Program Operating Manual
NTK	Need-To-Know
OPM	Office of Personnel Management
PCL	Personnel (Security) Clearance
POC	Point of Contact
PR	Periodic Reinvestigation
PSMO-I	*(See VRO)* Personnel Security Management Office for Industry
RD	Restricted Data
S	SECRET
SAP	Special Access Program
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SMO	Senior Management Official
SPP	Standard Practices and Procedures
TS	TOP SECRET
U	Unclassified
USG	United Stated Government
VAL	Visit Authorization Letter

VAR	Visit Authorization Request
VRO	Vetting Risk Operations

24. Forms & Systems

ACCS	Army Centralized Contracts and Security Portal
DD Form 254	Department of Defense Contract Security Classification Specification
DISS	Defense Information System for Security
DISS JVS	Defense Information System for Security (Joint Verification System)
DISS PSSAR	Personnel Security System Access Request DCSA (DD Form 2962, Vol 2)
NBIS	National Background Investigation Services
NBIS PSSAR	Personnel Security System Access Request DCSA (DD Form 2962, Vol 2)
NISS	National Industrial Security System
SF-312 (NDA)	Standard Form 312 (Non-Disclosure Agreement)
SF-86	Standard Form 86 / Questionnaire for National Security Positions
SF-85/SF-85P	Standard Form 85 / Questionnaire for Non-Sensitive Positions/Questionnaire for Public Trust Positions
SWFT	Secure Web Fingerprint Transmission

25. References

32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM)

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.)
   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)

2. Unofficial contact with a known or suspected foreign intelligence entity:
   a) Service(s) involved
   b) Name of individual(s) contacted
   c) Date(s) of contact
   d) Nature of contact to include any unusual or suspicious activity
   e) Likelihood of future contacts

3. Continuing association with a known foreign national(s) or foreign national roommate(s):
   a) Name of foreign national(s)
   b) Citizenship(s)
   c) Occupation
   d) Nature of relationship, i.e., business or personal
   e) Duration and frequency of contact(s)
   f) Current status of the relationship(s)

4. Involvement in foreign business:
   a) Nature of involvement
   b) Countries involved
   c) Name of business

5. Foreign Bank Account:
   a) Financial institution
   b) Country

6. Ownership of foreign property:
   a) Location
   b) Estimated value
   c) Balance due

d) Purpose and use of property
e) How acquired

7. Foreign citizenship:
   a) Country
   b) Basis for citizenship
   c) Date of application or receipt

8. Application for a foreign passport or identity card for travel:
   a) Country
   b) Date of application
   c) Reason for application

9. Possession of a foreign passport or identity card for travel:
   a) Issuing country
   b) Number
   c) Date of issuance
   d) Expiration date
   e) Reason for possession

10. Use of a foreign passport or identity card for travel:
    a) Issuing country
    b) Reason for use
    c) Date(s) and country(ies) of use

11. Voting in a foreign election:
    a) Date
    b) Country
    c) Election

12. Adoption of non-U.S. citizen children:
    a) Country involved
    b) Foreign government organization involved
    c) Foreign travel required
    d) Adoption agency or other intermediary
    e) Adoptive parents' current linkage to foreign country

13. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure:
    a) Date(s) of incident
    b) Name of individual(s) involved
    c) Nature of incident
    d) Method of contact
    e) Electronic address
    f) Type of information being sought
    g) Background, circumstances, and current state of the matter

14. Media contacts:
    a) Date(s) of contact

b) Name of media outlet
c) Name of media representative
d) Nature and purpose of contact
e) Whether classified information or other information specifically prohibited by law from disclosure was involved in the contact
f) Current status of the contact

15. Arrests:
    a) Date(s) of the incident(s)
    b) Location(s) of the incident(s)
    c) Charges and/or circumstances
    d) Disposition

16. Financial Issues and Anomalies:
    a) Type of issue or anomaly (bankruptcy, inheritance, etc.)
    b) Dollar value
    c) Reason

17. Cohabitant(s):
    a) Name(s)
    b) Citizenship(s)
    c) Date of Birth
    d) Place of Birth
    e) Duration of contact(s)

18. Marriage:
    a) Name of spouse
    b) Citizenship of spouse
    c) Date of Birth
    d) Place of Birth
    e) Date of marriage

19. Alcohol- and drug-related treatment:
    a) Reason
    b) Treatment provider, to include contact information
    c) Date(s) treatment provided