STANDARD PRACTICES AND PROCEDURES (SPP)

Index Systems Inc
13503 Copper Bed Road
Herndon VA 20171
750D4

Forward

Our Company has entered into a Security Agreement with the Department of Defense (DoD) in order to have access to information that has been classified because of 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 in the Government Manual – the National Industrial Security Program Operating Manual (NISPOM). The purpose of our SPP is to provide our Employees with the requirements of the NISPOM as they relate to the type of work we do. This document should also serve as an easy reference when questions about security arise. The NISPOM is available for review by contacting the Facility Security Officer (FSO) or through the Security Control (Sec-Con) Employee Portal.

Our Company fully supports the National Industrial Security Program (NISP). All of us have an obligation to ensure that our security practices contribute to the security of our Nation's classified defense information.

Table of Contents

1. Introduction....1

2. Facility Information....1

2.1. Facility Clearance....1

2.2. Facility Security Officer....1

2.3. Detailed Threat Report....1

2.4. Company Assets....1

2.5. Government Customers....1

3. Security Education....2

3.1. Initial Security Briefings....2

3.2. Annual Security Briefings....2

3.3. Debriefings....2

3.4. Derivative Classification Training....2

4. Security Vulnerability Assessments/Self-Inspections....2

4.1. Defense Counterintelligence and Security Agency....2

4.2. Security Vulnerability Assessments and other Assessments....2

4.3. Self-Inspections....3

5. Individual Reporting Responsibilities....3

5.1. Espionage/Sabotage....3

5.2. Suspicious Contacts....3

5.3. Adverse Information....3

5.4. Loss, Compromise, or Suspected Compromise of Classified Information....4

5.5. Security Violations....4

5.6. Personal Changes....4

5.7. Security Equipment Vulnerabilities....4

6. Graduated Scale of Disciplinary Actions....4

7. Defense Hotline....5

8. Marking Classified Information....6

8.1. Classification Levels....6

8.2. Original Classification....6

8.3. Derivative Classification....6
9. Classified Discussions....6
10. Public Release/Disclosure....6
11. New Hire and Onboarding Process....6
11.1. Initial Human Resources Responsibilities....7
11.2. Initial Security Team Responsibilities....7
12. Change in Employee Status....8
13. Security Access Validations....8
14. Separations and Terminations....8
15. JPAS Account Procedures....9
15.1. IsI Internal Accounts....9
15.2. IsI External Client Accounts....9
15.3. Client Accounts....10
16. DISS Account Procedures....10
16.1 IsI Internal Accounts....10
16.2 IsI External Client Accounts....10
16.3 Client Accounts....10
17. National Industrial Security System Account Procedures....11
17.1. IsI Internal Accounts....11
17.2. IsI External Client Accounts....11
18. Visit Procedures....11
18.1. Incoming Visits....11
18.2. Outgoing Visits....11
18.3. Entering an Outgoing Visit Request in JPAS....11
18.4. Modifying or Canceling a Visit Request in JPAS....12
19. Initiating an Investigation in e-QIP....12
19.1. Investigations....12
19.2. Initiating the investigation in e-QIP....12
20. Special and Caveated Accesses....14
21. Emergency Procedures....14
21.1. Emergency Plan....14

21.2. Emergency Contact Numbers....14
22. Security Team Operations and Job Functions....14
22.1. Operations....14
22.2. Security Team Organization Chart and Structure....15
22.3. Security Team Job Functions....15
23. Definitions....18
24. Abbreviations and Acronyms....19
25. References....21
26. Addendum A – Threat Analysis and Mitigation Plan....21
27. Addendum B - Safeguarding of Classified Materials....21

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 NISPOM26, 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 NISP.

Additional Specific Operating Procedures (SOP) may be attached to this 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) for our Employee so they can perform on classified contracts. Please reach out the Security Team 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 Security Awareness Briefing.

2.2. Facility Security Officer

As a result of having an FCL, we agree to adhere to the rules of the NISP. As part of the NISP, Contractors are responsible for appointing a Facility Security Officer (FSO). The FSO must be a United States citizen, an Employee of the Company, and cleared to the level of FCL. The FSO must complete all required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM and the related Federal requirements for classified information. The contact information for the FSO, the Insider Threat Program Security Officer (ITPSO) and the Security Teams is in Sec-Con on the front page of your Employee Security Dashboard. Anytime the FSO or their contact information changes or is updated, it will be posted in Sec-Con. You will receive automated email notifications of any contact changes.

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 and Security Agency (DCSA). These reports will be used to identify threats specific to our business and help identify Company assets that need protection.

2.4. Company Assets

Our Company assets are identified in Addendum A – Threats, Assets, and Mitigation. This asset list is a work in progress and will also encompass the Threat Protection Plan.

2.5. Government Customers

Our Government Customers are responsible for providing us 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

All cleared Employees must receive an initial security briefing and sign a Classified Information Nondisclosure Agreement (SF-312) prior to being granted access to classified material for the first time. The SF-312 is an agreement between the United States and a cleared individual. At a minimum, the initial briefing will include the following:

- Threat Awareness Briefing.
- Defensive Security Briefing.
- Overview of Security Classification System.
- Employee reporting obligations and requirements.
- Overview of the SPP.

3.2. Annual Security Briefings

Annual briefings will be provided to all cleared Employees to remind them of their obligation to protect classified information and provide any updates to security requirements and potential threats.

These training courses will be issued via Sec-Con when possible by the Security Team.

3.3. Debriefings

When a cleared Employee no longer requires a security clearance, access to classified information, or terminates employment with our Company, the Security Team will debrief the Employee.

These debriefs will be administered by the Security Team via Sec-Con.

3.4. Derivative Classification Training

Employees who have been authorized to make derivative classification decisions must complete initial derivative classification training, and 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 whether initial or refresher. Contact the Security Team for guidance on how to access and complete the training.

4. Security Vulnerability Assessments/Self-Inspections

4.1. Defense Counterintelligence and Security Agency

DCSA is the Government Cognizant Security Office (CSO) 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 Vulnerability Assessment (SVA) or continuous monitoring 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.

Please contact any of your security Points of Contact (POC) in Sec-Con for the name, address, email address and phone number of our DCSA ISR and/or Counter Intelligence (CI) Representative as their information may change frequently.

4.2. Security Vulnerability Assessments and other Assessments

DCSA does not have a set schedule of when they are going to conduct an assessment or continuous monitoring review of the facility. During these assessments, DCSA ISRs will review our security practices and procedures to ensure compliance with the NISPOM and interview our Employees to assess the effectiveness of the security program. Your cooperation with DCSA during the SVA is required.

4.3. Self-Inspections

Our Security Team will perform a Self-Inspection, similar to the DCSA SVA, at least once every twelve months. The purpose of a Self-Inspection is to identify any vulnerabilities in our security procedures, to determine the effectiveness and identify any deficiencies/weaknesses in our practices and procedures to better determine the effectiveness of our security procedures. As part of this Self-Inspection, Employees will be interviewed. The results of the Self-Inspection will be provided to DCSA for review. Self-Inspections 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 the Executive Management Team and/or Senior Management Official.

Each Self-Inspection will contain interviews of Employees. The number of interviews to be conducted will be as follows:

- For companies less than 25 Employees = 100% interviews.
- For companies more than 25 Employees and less than 50 Employees = 50% interviews.
- For companies more than 50 Employees and less than 100 Employees = 25% interviews.
- For companies more than 100 Employees = 10% interviews.
- For companies more than 500 Employees = will be determined based on additional guidance.

5. Individual Reporting Responsibilities

Contact information for our Security Team can be found in your Employee Security Portal in Sec-Con. All Employees are to report any of the following information to the Security Team. These reports will be initiated in Sec-Con for the purposes of tracking and compliance.

5.1. 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.

5.2. 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.

5.3. Adverse Information

Adverse information is any information regarding a cleared Employee, or an Employee 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 Department of Defense Consolidated Adjudications Facility (DoD CAF) via Joint Personnel Adjudication System (JPAS)/ 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.
- Excessive debt, including garnishments of Employee's wages.
- 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 United States 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.

5.4. 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 notify DCSA immediately 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 of this could be an individual's personal cell phone with email capability that received a classified email by mistake.

5.5. Security Violations

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

5.6. Personal Changes

Cleared personnel must report personal changes to the Security Team to include but not limited to:

- Change in name.
- Termination of employment/Leave of Absence (LoA).
- Change in employment type.
- Change in citizenship.
- Access to classified information is no longer needed.
- No longer wish to be processed for a personnel clearance or continue an existing clearance.

5.7. Security Equipment Vulnerabilities

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.

6. Graduated Scale of Disciplinary Actions

Contractors will establish and enforce policies that provide for appropriate administrative actions taken against Employees who violate requirements of this Manual. They will establish and apply a graduated scale of disciplinary actions in the event of Employee violations or negligence. A statement of the administrative actions taken against an Employee will be included in a report to the Cognizant Security Agency (CSA) when individual responsibility for a security violation can be determined, and one (1) or more of the following factors are evident:

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

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

The Company has established a graduated scale of administrative sanctions up to and including dismissal from employment. As a rule, the FSO may recommend an appropriate sanction; however, Senior Leadership will make the final determination of the sanction to be administered.

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

The following provides a uniform application of the administrative actions for a first offense procedural infraction committed within a three (3) year period:

- A verbal reprimand provided by the FSO, and a refresher briefing provided by the Security Team.
- A written reprimand signed by the FSO and placed in the individual's PCL record.
- A suspension of access to classified materials and restricted areas will be made by the FSO if determined appropriate to the infraction.
- A suspension without pay for a period of one (1) week, and a reassessment of the continued employment of the person, or persons in a position requiring access to classified information made by the Senior Leadership in consultation with the FSO if determined appropriate to the infraction.

For a second offense committed within a three (3) year period:

- A verbal reprimand by the FSO with a warning of further disciplinary action for any future incidents. A refresher brief provided by the Security Team.
- A written reprimand provided by the FSO and placed in the individual's PCL record.
- A suspension of access to classified materials and restricted areas will be made by the FSO if determined appropriate to the infraction.
- A suspension without pay for a period of one (1) week and a reassessment of the continued employment of the person or persons in a position requiring access to classified information made by the Executive Leadership in consultation with the FSO if determined appropriate to the infraction.

For a third offense committed within a three (3) year period:

- Verbal reprimand accompanied by a written reprimand provided and signed by the FSO will be placed in the individual's PCL record along with a stern warning of consequences for a future offense
- A written reprimand signed by the FSO and placed in the individual's PCL record.
- A refresher brief specific to the security incident provided by the Security Team.
- A suspension of access to classified materials and restricted areas will be made by the FSO in consultation with the Senior Leadership if determined appropriate to the infraction.
- A suspension without pay for a period of one (1) week and a reassessment of the continued employment of the person or persons in a position requiring access to classified information made by Senior in consultation with the FSO if determined appropriate to the infraction.

The FSO and ITPSO reserve 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 the FSO or ITPSO identify that the individual is a serious threat to National Security, they may, without authority from any other Senior Leadership, terminate the individual's access to classified materials at any time pending a review by the company and CSA.

7. 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 as well as other hotline numbers are available to you in your Sec-Con Employee Security Portal.

DEFENSE HOTLINE

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

8. Marking Classified Information

8.1. 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 "Identifiable" damage to National Security.

8.2. 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.

8.3. Derivative Classification

Employees authorized to perform derivative classification actions must have adequate training, and the proper Security Classification Guides (SCG) and/or guidance necessary to accomplish these important actions.

9. 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 will only be done at cleared sites.

10. Public Release/Disclosure

Our Company 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.

11. New Hire and Onboarding Process

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

11.1. Initial Human Resources Responsibilities

Upon receipt of acceptance of an Offer Letter for a new Employee, HR will enter the new hire information into Sec-Con. The HR Team will identify the specific contract(s) the Employee is supporting, the highest level of security access required, and what computer system accesses are required. Once the information is entered into Sec-Con, the Security Team will receive a notification on the new hire in Sec-Con and via email.

11.2. Initial Security Team Responsibilities

All new hires who have an existing or pending clearance, a requirement to have to classified materials, or a system that requires eligibility (JPAS, DISS etc.), and have an active contract they support will require an onboarding meeting with the Security Team. Please note that this meeting can be virtual.

During the onboarding meeting, the Security Team will gather the following documents, to include but not limited to:

- SF-312.
- Initial Security Awareness Training Certificate.
- Proof of United States Citizenship (if an investigation or reinvestigation is required).
- A Type A Consulting Certificate (if the new hire is a Form 1099 Individual Consultant).

All new hires who do not have a clearance and require a new SF-86 for eligibility, in addition to above will:

- Complete an SF-86 via Electronic Questionnaires for Investigation Process (e-QIP).
- Execute and provide a signed copy of the Privacy Act Statement.

When entering a new hire in JPAS, the following actions will 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 in JPAS 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".
    - The Assistant Facility Security Officer (AFSO) will get guidance from DCSA on how they want to see subcontractors if the Government Contracting Activity (GCA) is requiring subcontractors to be in the Personnel Security Management Network (PSM Net) under the prime contractor and on a Joint Visit Request. Any such guidance from will be saved in Sec-Con under the NISPOM Waivers section.
- AFSO will take an "owning" relationship with the individual if they are a Form W-2 Employee and will take a "servicing" relationship if the individual is a Form 1099 Independent Contractor.
- AFSO will insert an "In Processing Date" in JPAS. ** An In-Processing Date will NEVER be back dated.
- AFSO will insert a date at the appropriate access level as determined by the Security Team and Manager.
- All information pertaining to an individual's JPAS record will be entered in Sec-Con.

12. Change in Employee Status

HR or the Employee will report, via Sec-Con, any of the following Employee status changes.

- Change in Name
    - A name change will require supporting documentation of the change. The Security Team will modify JPAS with the new name and provide supporting documentation to Personnel Security Management Office for Industry (PSMO-I).
- Change in Employment Status (New Hire, Separating, LoA, Leave without Pay (LWOP):
    - For Employees separating, the Security Team will follow the separation procedures in Section 14.
    - Any Employee on LoA or LWOP, will have their access in JPAS removed pending the resolution of status.
- Change in Contract
    - The Security Team will 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 will be modified to meet the current requirements.
- Change in Job Position/Title
    - The Security Team will 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 will be modified to meet the current requirements.

13. Security Access Validations

Access levels in JPAS will be conducted and validated on an ongoing basis. The Security Team will meet with the Controller, HR, Manager, or the appropriate individuals to review the current list of Employees and/or Consultants by comparing the JPAS PSM Net report to the payroll report and with the current access requirements the Manager provides for that period.

The Manager will be prepared to provide the contract number and highest level of classification required for each individual who is in the PSM Net.

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

Employees who only require access to JPAS/DISS but are not actively accessing classified materials, will be owned or serviced in the JPAS PSM Net without being indoctrinated. Although they will not be indoctrinated, they will still be required to follow all rules and requirements set forth as a cleared Employee.

14. Separations and Terminations

The Manager will notify HR upon any termination or resignation immediately and will enter that information into Sec-Con (provided HR has not already entered it).

The Employee will then meet with the Security Team to begin the Out-Processing.

The Security Team will ensure the following actions occur:

- In JPAS the indoctrination level is removed, an Out-Processing date is entered, and a separation date is entered with the appropriate category. ** At no time will the Out-Processing date, or separation date be back or postdated without express authority of the DCSA and/or a Federal Judge.

- "Separation" will be used for any Employee who 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. For each Employee's record that an Invalid entry was entered in JPAS, a note will be placed in the Sec-Con Employee file.
- "Facility Termination" will only be used by the government upon the FCL being inactivated.

- The Employee will complete the debriefing section of the SF-312 or similar form.
- The Employee will certify that they have returned all equipment and proprietary information (if required).
- The Employee's physical access to the building will be deactivated and/or removed.
- The Employee's Sec-Con record will be set to inactive with a separation date.
- The Security Team will remove all JPAS Accounts associated with the Employee and notify any Clients who will be required to remove JPAS access as well.

15. JPAS Account Procedures

There are three (3) types of accounts Employees may require.

15.1. IsI Internal Accounts

When an Employee requires an IsI JPAS Account (CAGE Code 68DV9), the following procedures will be followed:

The Security Team Lead assigned to the CAGE Code will prepare a Personnel Security System Access Request (PSSAR) with the requirements from the individual's Manager. JPAS Accounts will be determined to be a Level 3, 4, 5, or 6 depending on the access required. The Top Hierarchy Account Manager (AM) will review the PSSAR and meet with the Manager to confirm the requirement and execute the PSSAR. Should an individual require AM privileges under this CAGE Code, the individual must be a Form W-2 Employee, and the FSO must have written approval from the Chief Executive Officer (CEO) and the President. In the absence of the CEO or President, a second Executive Manager (excluding the FSO) can approve this access. There will always be the JPAS Top Hierarchy AM plus two-person integrity by the Executive Management Team to approve AM Status for JPAS.

For the Primary Top Hierarchy AM, the PSSAR, required training certificates and Letter of Appointment (LOA) will be submitted to Defense Manpower Data Center (DMDC) for processing.

IsI mandates that all Employees requiring access to JPAS complete refresher JPAS training, certify they have read the JPAS User Policy, and JPAS AM Policy prior to being granted access.

15.2. IsI External Client Accounts

When an Employee requires a Client JPAS Account, the following procedures will be followed:

The Transition Specialist (for new Clients in transition), the Security Team Lead (for existing Clients), or the FCL Team (for companies initially receiving their FCL) assigned to the CAGE Code(s) will prepare a PSSAR with the requirements from the individual's Manager. JPAS Accounts will be Level 3, 4, 5, or 6 depending on the access required. **AT NO TIME WILL THE ROLE OF AM BE AUTHORIZED FOR AN ISI EMPLOYEE.** The PSSAR and training certificates will be submitted by the FCL Specialist to the Client Top Hierarchy AM for review, approval and execution. Upon submission of this form, the FCL Specialist will verbally discuss the PSSAR, and the requested access with the Client Top Hierarchy AM to alleviate any misunderstandings. The Client Top Hierarchy AM will be responsible for setting up the JPAS Account.

Clients will "service" not "own" IsI personnel requiring access to JPAS in their PSM Net. At no time will an IsI Employee be "Indoctrinated" with an access level, unless a specific Government Agency requires such action. For example, Sensitive Compartmented Information (SCI) Indoctrination.

15.3. Client Accounts

Only Clients are authorized to have AM Status in JPAS. AM Accounts will be coordinated with DMDC. Each Client will have an AM and Secondary AM.

16. DISS Account Procedures

Employees may require one (1) of the following accounts:

16.1 IsI Internal Accounts

When an Employee requires an IsI DISS Account (CAGE Code 68DV9), the following procedures will be followed:

The Security Team Lead assigned to the CAGE Code will prepare a PSSAR with the requirements from the individual's Manager. DISS/Joint Verification System (JVS) Accounts will be issued as a "Security Officer" Role. The Top Hierarchy AM will review and meet with the Manager to confirm the requirement and execute the PSSAR form. Should an individual require AM privileges under this CAGE Code, the individual must be a Form W-2 Employee, and the FSO must have written approval from the CEO and President. In the absence of the CEO and President, a second Executive Manager (excluding the FSO) can approve this access. There will always be the DISS/ JVS Top Hierarchy AM plus two-person integrity by the IsI Executive Management Team to approve the AM Status for JPAS.

For the Primary Top Hierarchy AM, the PSSAR, required training certificates, and LOA will be submitted to DMDC for processing.

IsI mandates that all Employees complete the required trainings referenced in the JVS User Manual, the Annual Refresher Trainings, and certify they have read the DISS/JVS Account Management Policy prior to being granted access.

16.2 IsI External Client Accounts

When an Employee requires a Client DISS/JVS Account, the following procedures will be followed:

The Transition Specialist (for new Clients in transition), the Security Team Lead (for existing Clients), or the FCL Team (for companies initially receiving their FCL) assigned to the CAGE Code will prepare a PSSAR with the requirements from the individual's Manager. JPAS Accounts will be issued as a "Security Officer". The PSSAR form and training certificates will be submitted by the FCL Specialist to the Client Top Hierarchy AM for review, approval, and execution. Upon submission of this form, the Change Condition Specialist (for new Clients in transition) or the Security Team Lead (for existing Clients) will verbally discuss the PSSAR, and the requested access with the Client Top Hierarchy AM to alleviate any misunderstandings. The Client Top Hierarchy AM will be responsible for setting up the DISS/JVS Account.

Clients will "service" not "own" IsI personnel requiring access to DISS/JVS in their PSM Net. At no time will an IsI Employee be "Indoctrinated" with an access level, unless a specific Government Agency requires such action. For example, SCI Indoctrination.

16.3 Client Accounts

Clients will be required to maintain at least one (1) Top Hierarchy AM account and the Senior Management Official will be required to have a Key Management Personnel (KMP) Account.

17. National Industrial Security System Account Procedures

There are two (2) types of accounts that Employees may require:

17.1. IsI Internal Accounts

When an IsI Employee requires an IsI NISS Account under CAGE Code 68DV9, the Employee will go to the NISP Central Access Information Security System (NCAISS) system and request a National Industrial Security System (NISS) Account. Once that is complete the Employee will notify the IsI FSO that an account has been requested. Once the FSO approves the request, the FSO will send an email to the DCSA ISR requesting they approve the account.

17.2. IsI External Client Accounts

When an IsI Employee requires an IsI NISS Account under a Client, the Employee will go to the NCAISS system and request a NISS Account. Once that is complete the Employee will notify the Client FSO that an account has been requested. Once the Client FSO approves the request, the Client FSO will send an email to the DCSA ISR requesting they approve the account.

18. Visit Procedures

18.1. Incoming Visits

All incoming classified visits must be approved in advance of the visit by the Security Team. The Security Team will verify each visitor's security status 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 JPAS, 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, positive identification of the person must be accomplished.

Once a visitor has been identified and approved, the Security Team will enter this individual's Visit Request and clearance information into the Sec-Con Visitor Control Portal.

18.2. Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When it becomes necessary for Employees of IsI 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. Ample time must be allowed for the Visit Request to be prepared, submitted via JPAS to the Contractor/agency, and processed by their visitor control. All outgoing Visit Requests will be entered in the Outgoing Visit Request Module of Sec-Con.

18.3. Entering an Outgoing Visit Request in JPAS

- In JPAS, select the appropriate CAGE Code for which the Visit Request is being processed.
- Click "Create/Modify Visit" on the Main Menu. The "Add/Modify/Cancel a Visit" screen appears.
- Click the "Add Visit" button.
- Select "Reason for Visit" and "Visit Access" from drop down menus (required).
- Enter the Point of Contact's (POC) name and phone number, then enter the visit dates.

- Enter any additional information, if required, in the additional information box.
- Click “Select SMO”; and the “Security Management Office Selection” screen appears.
- Enter the SMO code in the box and click ‘Search”.
- Select the appropriate SMO Code; and the “Visit Information” screen will reappear.
- Hit “Save” at the bottom of screen to save the SMO info.
- Now that the visit is saved you can add your visitor(s).
- Click “Add Visitor(s)”; and the “Person Category Search Screen” appears.
- Enter the visitor’s SSN then click “Search”; and the “Search Result Section” is populated.
- Click “Add Visitor” to add the SSN/Visitor to the “Visit Notification”.
- Click “Cancel”; and the “Visit Information” screen reappears with an updated “Visitor List”. The visiting organization will now be able to view visit request.

18.4. Modifying or Canceling a Visit Request in JPAS

Below are the procedures for modifying or deleting a Visit Request in JPAS. Please note: agencies that require Visit Requests to be processed outside of JPAS will require a Visit Termination Letter or Visit Modification Letter. From the Main Menu, click “Create/Modify Visit”; then the “Add/Modify/Cancel A Visit” screen appears.

- Select the SMO/Visit you wish to modify or cancel.
- The “Visit Information” screen appears.
- Select “Modify Visit” to make necessary modification(s).
- Select “Cancel Visit” to cancel the visit.
- Click “Save” to update and send the updated Visit Notification and/or cancellation.

All visit actions entered in JPAS or provided to an organization via other means will be entered in Sec-Con.

19. Initiating an Investigation in e-QIP

19.1. Investigations

All requested investigations and upgrades must be approved in advance of initiating the e-QIP by the FSO. The FSO will verify the Employee requires access and is on a supporting contract prior to initiating the e-QIP. Below are the procedures for initiating an investigation in JPAS through e-QIP.

19.2. Initiating the investigation in e-QIP

- To request an investigation, you must first have e-QIP permissions granted by an AM.
- Click the “Investigation Request” link located below the “In/Out Process” hyperlink.
    - Ensure the “Correct Person Category” is displayed.
    - Ensure you have a relationship with the person.
    - Check “Investigation Summary” section for an active investigation request.
- Select the “Investigation Request” link to get to the “Determine Investigation” screen.
- From the “Determine Investigation Screen”:
    - Select “Eligibility” from the drop down menu, click “Determine Investigation Type” to get to the “Initiation Scope” screen.
    - “New Investigation Types” of T3 for initial Confidential and Secret; T3R for Confidential and Secret Periodic Reinvestigations (PR); T5 for initial TS and T5R for TS Reinvestigations.
    - JPAS users can indicate when a “Break in Service” has occurred.
        - “Break in Service” allows a new “Investigation Request” to be initiated even though a person may already have a current investigation date.
        - Check the “Break in Service” box (if required) to continue the request.
- Investigation request.
    - Enter the contract number on the “Initiation Scope Screen”.
    - A contract number is required for each “Investigation Request”.

- A contract number must include the identification of the Government Customer requiring the PCL as well as the contract number itself.
- Do not type "various" or "multiple" or "unknown" in this field.
- The correct standardized format for a contract number is as follows:
  - When writing the contract number include the full contract number in all capital letters.
    - *For example: NAVY N0001906D0014*
  - If the contract number is classified, still list the contracting agency then list the type of classification. (CLASSIFIED, CIRCLE A, YANEE WHITE, etc.). If the agency is also classified just list CLASSIFIED.
    - *For example: DHS CLASSIFIED or if the agency is classified as well: CLASSIFIED*
  - If the person requesting the investigation works on multiple contracts, list their primary contracting agency and contract number.
  - When requesting an investigation for SCI or Special Access Program (SAP) access, include "SCI" or "SAP" between the name of the Government Customer and the contract number.
    - *For example: NAVY SAP N0001906D0014*
  - Investigations for a KMP of a cleared company should reflect the Contractor's primary classified contract and associated Government Customer.
- Additional Scope information screen.
  - Click "Calendar" and enter the "Local Agency Check Date". It is the date you initiate the investigation.
  - Enter the Submitting Office Number (SON): 346W.
  - Enter the Security Office Identifier (SOI): DD03.
  - Click drop down on "Access/Eligibility" and choose the clearance level you are initiating the investigation on.
  - Choose the drop down in "Applicant Affiliation": You will choose "Contractor".
- If fingerprints are required, then select "Fingerprints will be electronically sent".
- On the "Additional Request Information" screen select "Requesting Official"
  - Provide your Name.
  - Title.
  - Email address.
  - Phone number.
- Choose "Initiate PSI".
- Click "Save" or "Save and Return".

- Investigation Initiated.
  - Once the investigation request has been initiated, you will see a notification on the "Person Summary Screen" (Investigation Summary).
  - You will also receive a notification via the "Investigation Request Status Notification" screen.
  - You will receive a "Registration Code" via "Message From CAF".
  - You will need to inform the applicant, provide the "Registration Code" and instructions on how to begin the e-QIP process.
  - Once the applicant completes the investigation, and the e-QIP has been released back to the requestor, the AFSO will review the SF-86 and submit the investigation to PSMO-I for "Review/Approval".

Once initiated and submitted to PSMO-I, the FSO will enter the individual's initiated investigation information into their Sec-Con profile.

***Note: In the email to the applicant please add: Please note the Security Team will review your SF-86 (investigation request) for accuracy and completion ONLY and information contained within that document is subject to Section 552a of title 5, United States Privacy Code also known as the**
Privacy Act of 1974. Your personal information will not be utilized for any other purposes within the Company.

20. Special and Caveated Accesses

The FSO will verify all requested "Special and Caveated" accesses, e.g. 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 ISR of DCSA before briefing any Employee.

Once the FSO is briefed by the CSA, the Employees may be briefed. Initial briefings and refresher briefings will be maintained in Sec-Con.

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 will follow Intelligence Community (IC) directives, policy guidance, standards, and specifications for the protection of classified national intelligence and SCI.

21. Emergency Procedures

21.1. Emergency Plan

In emergency situations, it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency is the safety of personnel. Do not risk your life or the lives of others in order 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.

21.2. Emergency Contact Numbers

The Emergency POCs are the same as our security POCs. A list of the most current contact information for these individuals is in Sec-Con under your Employee Security Dashboard. As these individuals and/or their contact information may change frequently, you will receive an automated email from Sec-Con anytime there is a change to the emergency contact list.

22. Security Team Operations and Job Functions

22.1. Operations

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

Internally we will maintain at a minimum the following positions:

- Facility Security Office (FSO).
- Insider Threat Program Security Officer (ITPSO).

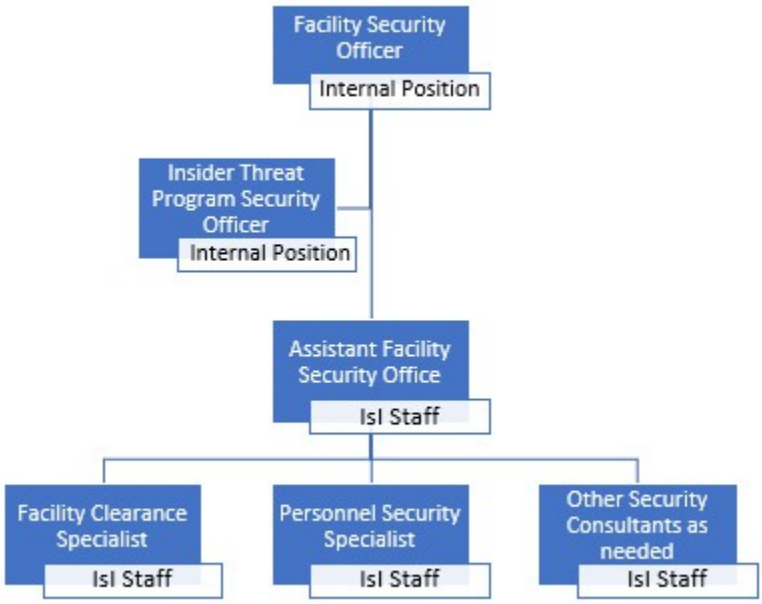
External individuals (from IsI) supplementing our internal team shall consist of:

- Assistant Facility Security Officer (AFSO).
- A Personnel Security Specialist (PSS).
- A Facility Clearance Specialist.
- 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 IsI support staff will prepare all paperwork for review and approval by the FSO as well as taking all actions as required in JPAS/DISS/NISS.

22.2. Security Team Organization Chart and Structure

Below is an Organizational Chart of the security staff who will be supporting this role.



22.3. Security Team Job Functions

Below are the job specific functions of each role.

FSO

- The FSO will provide all leadership and direction on behalf of the company for the security program. They will be the main interface between difficult 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.

ITPSO

- 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 receive will be reported to the Senior Management Official and DCSA in a timely manner.

AFSO (IsI)

- The AFSO will be the lead IsI security person and will report directly to the FSO. They will be responsible for the following actions:
  - Ensure all security staff personnel are maintaining their access to JPAS and DISS.
  - Supervise and direct security measures necessary for implementing applicable requirements for the NISPOM and related Federal requirements for classified information.
  - Maintain all initial and periodic re-investigation security clearance investigations. This can be handled by the PSS based on their confidence and experience with JPAS and knowledge of the process.

- Ensure the Team is conducting initial security briefings for all new Employees followed by annual refresher briefings.
- Keep the FSO and the Employees informed of potential threats to security, including cyber intrusions on unclassified systems, and understand special requirements for handling certain types of classified information.
- If requested, provide guidance on safeguarding classified materials from unauthorized disclosure.
- Provide contract specific security training as needed.
- Based on the Client's guidance, the Security Team may be responsible for reporting to the Government specific types of actions, situations, or status changes relating to the potential compromise of classified information and/or unclassified information relating to the Clients classified programs, to include cyber intrusions on your unclassified systems.
- Report adverse information, suspicious contacts, foreign contacts, insider threats, etc.
- Report all matters related to FCL changes/updates to FCL specialist which are not related to security/incident reports.
- Acts as the main POC and interface for their Client.
- Check JPAS notifications twice daily and process accordingly. Additionally, inform the Clients and/or Employees of all changes related to their security profiles.
- Employees should be informed of eligibility updates immediately (same day) and indoctrinate accordingly.
- Review employee's SF-85/SF-86 for accuracy and completeness then submit to the appropriate Government agency for their review and approval.
- Process all Sec-Con requests from Clients, e.g. new hires, Visit Requests, Foreign Travel Briefings, etc. and delegate to PSS accordingly.
- Process new hires in JPAS, DISS, Sec-Con, and additional security databases (e.g. SPOT, ACCS) accordingly. Pick up the Employee's collateral clearances/initiate clearance investigations.
- Prepare and process all Linguist Packets/SIP packages/SCI nominations to be submitted to the appropriate agency *(if not already carved out of the contract)*.
- Process and submit CAC card requests/TASS actions to the appropriate agency for processing per the guidance of the security POC associated with the DD Form 254.
- Assist Clients in the preparation and completion DCSA SVA/CE's. This may require travel to various locations throughout the United States and its territories.
- Track and maintain all requested documents with the assistance of the PSS and Sec-Con database.
- Administer Foreign Travel Briefings/Debriefings for cleared Employees going on unofficial foreign travel. If required, submit these Foreign Travel Briefings to the appropriate SSO for visibility.
- Delegate tasks to the PSS and Facility Clearance Specialist as needed.
- Contact the PSMO-I with personnel security related questions or concerns.
- Submit all DD Form 254s to Client/CM/COR for review and approval.

Personnel Security Specialist (IsI)

- The PSS will be the main individual responsible for administrative security duties. This individual will take their direction from the AFSO and ultimately the FSO. They will be responsible for the following actions:
  - Update and maintain data and documents in Sec-Con JPAS/DISS.

- Acknowledge email and upload all necessary documents (e.g. NDA, trainings, completed NATO/ COMSEC documents, etc.) and add all related document data into Sec-Con accordingly.
- Add/update information given from their Security Team and Management Team.
- Send welcome/new hire/investigation initiation email with required documents to include instructions on how to complete the request/documents.
- Administer all required annual trainings/briefings.
- Assist the Security Lead with all indoctrinations/debriefs and JPAS personnel reports. Send NDA for completion if it's an initial indoctrination (never had a clearance).
- Submit Visit Requests/visitor termination requests via JPAS, ACCS or email for paper Visit Requests. Additionally, the PSS is tasked with uploading all Visit Request information into the visit request portion of Sec-Con. Once completed, ensure all appropriate visit information/documents is added in Sec-Con.
- In/out process Employees per the request of the Security Lead/Clients.
- Assist the Security Team when constructing new DD Form 254s. Upload the completed (signed by CM/COR) DD Form 254 and data into Sec-Con.
- Ensure data integrity in all security databases as it relates to clearance and personal information.
- Upload all documents as they are received from Clients and respond with an acknowledgement email, within one (1) hour.
- Assist the Security Lead with the overall responsibility and accountability for the assigned projects against pre-established timelines.
- Other duties as assigned by the AFSO or Management based on availability.
- The only time a PSS will initiate a security investigation, construct a DD Form 254, process a SCI nomination/Linguist Packet/SIP package, or other task that would normally be processed by a Security Lead, is per the guidance of the Security Lead or a member of the Management Team.

Facility Clearance Specialist

- Conduct periodic reviews of all CAGE Codes in Sec-Con to ensure data is correct and facility documents are compliant.
- Maintain cognizance of all actions being taken in NISS by the Facility Clearance Specialist. Review all NISS packages before they are submitted.
- Work with Clients and Security Team, as needed, to obtain all required documents for a Facility Clearance Sponsorship/Facility Clearance Upgrade/Facility Clearance Downgrade/Safeguarding Packages for all assigned CAGE Codes.
    - Sponsorship Letter.
    - DD Form 254.
    - Statement of Work (SOW)/Performance Work Statement (PWS).
    - Nomination Letter (if required).
- Monitor progression of Sponsorship Packages and call FCB for updates as needed.
- Work with Clients and the Security Teams, as needed, to conduct and certify Self-Inspections for all assigned CAGE Codes.
    - Complete the DCSA Self-Inspection Handbook using data in Sec-Con.
    - Review vulnerabilities with the Security Team.

- Provide a completed DCSA Self-Inspection handbook and schedule a call with the Client and the Security Team to review the DCSA Self-Inspection handbook and discuss vulnerabilities.
- Complete Employee questionnaires.
- Complete Certification Letter and provide it to the SMO for signature.
- Combine all Self-Inspection documents: Certification Letter, Handbook, and Questionnaires. Upload the combined document to Sec-Con.
- Certify the Self-Inspections are complete in NISS.
- Notify the FSO once certification is completed in NISS.

- Work with Clients and the Security Teams, as needed, to submit annual Personnel Security Investigation (PSI) projections for all assigned CAGE Codes.
  - Obtain data for PSI Projection chart.
  - Discuss data with the Client and the Security Team.
  - Insert data into NISS and submit the projection.
  - Provide a copy of the projection to the client.
- Work with the Clients and Security Teams, as needed, to submit Change Conditions for all assigned CAGE Codes.
  - Obtain required information to prepare templated documents required for the package.
  - Work with the Client to obtain signed copies of the required documents.
  - Upload information/documentation to NISS.
  - Have the Facility Clearance Assistant Manager review the package.
  - Submit the package.
  - Upload the documents and maintain notes, as required in Sec-Con.
  - Monitor the package for status changes.
  - Notify the Client once the package is approved and delete notes in Sec-Con
- Check NISS daily for updates to all assigned CAGE Codes. Upload the updated NISS data into Sec-Con, update the relevant fields in Sec-Con, and notify the Security Team of the updates.
- Track all open actions using the Change Condition Module and the notes section in Sec-Con.

23. 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 not be in the interest of National Security.
Authorized Person	A person who has a need-to-know for the classified information involved and has been granted a personnel clearance at the required level.

Classified Contract	Any contract that requires, or will require, access to classified information by the contractor or its Employees in the performance of the contract.
Classified Information	Official Government information which has been determined to require protection against unauthorized disclosure in the interest of National Security.
Cleared Employees	Employees granted a personnel clearance or who are in process for a personnel clearance.
Closed Area	An area that meets the requirements outlined in the NISPOM 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.
Communication Security (COMSEC)	COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications of the United States 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.
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 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 that could reasonably result in the loss or compromise of classified information.
Standard Practice Procedures (SPP)	A document prepared by contractors outlining the applicable requirements of the NISPOM 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.

24. Abbreviations and Acronyms

ACCS	Army Service Component Commands
AFSO	Assistant Facility Security Officer
AM	Account Manger
ASCC	Army Service Component Commands
CAC	Common Access Card
CAF	Consolidated Adjudications Facility

CAGE	Commercial and Government Entity
CE	Continuous Evaluation
CEO	Chief Executive Officer
CI	Counter Intelligence
CM	Contract Monitor
CNWDI	DoD Critical Nuclear Weapon Design Information
COMSEC	Communication Security
COO	Chief Compliance Officer
COR	Contracting Officer's Representative
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
DISS	Defense Information System for Security
DMDC	Defense Manpower Data Center
DNI	Director of National Intelligence
DoD	Department of Defense
DoD CAF	Department of Defense Central Adjudication Facility
DOE	Department of Energy
DCSA	Defense Counterintelligence and Security Agency
e-QIP	Electronic Questionnaires for Investigation Processing
FBI	Federal Bureau of Investigation
FCB	Facility Clearance Branch
FCL	Facility (Security) Clearance
FFP	Firm Fixed Price
FRD	Formerly Restricted Data
FSO	Facility Security Officer
GCA	Government Contracting Activity
HR	Human Resources
IC	Intelligence Community
ISR	Industrial Security Representative
ITPSO	Insider Threat Program Security Officer
JPAS	Joint Personnel Adjudication System
JVS	Joint Verification System
KMP	Key Management Personnel
LOA	Letter of Appointment
LoA	Leave of Absence
LWOP	Leave Without Pay
NATO	North Atlantic Treaty Organization
NCAISS	National Industrial Security Program (NISP) Central Access Information Security System
NDA	Non-disclosure Agreement
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISS	National Industrial Security System
NTK	Need-To-Know
OPM	Office of Personnel Management
PCL	Personnel Security Clearance
PKI	Public Key Infrastructure
POC	Point of Contact
PR	Periodic Reinvestigation
PSI	Personnel Security Investigation
PSM Net	Personnel Security Management Network
PSMO-I	Personnel Security Management Office for Industry

PSS	Personnel Security Specialist
PSSAR	Personnel Security System Access Request
PTO	Paid Time Off
PWS	Performance Work Statement
RD	Restricted Data
RFP	Request for Proposal
SAP	Special Access Program
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
Sec-Con	Security Control
SMO	Security Management Office
SOI	Security Office Identifier
SON	Submitting Office Number
SOP	Standard Operating Procedures
SOW	Statement of Work
SPOT	Synchronized Pre-deployment and Operational Tracker
SPP	Standard Practice Procedures
SSO	Special Security Officer
SVA	Security Vulnerability Assessments
TASS	Trusted Associate Sponsorship System
TS	Top Secret
USD(I)	Under Secretary of Defense Intelligence

25. References

[1] National Industrial Security Program Operating Manual (NISPOM), *DoD 5220.22-M*.

26. Addendum A – Threat Analysis and Mitigation Plan

The Threat Analysis and Mitigation Plan is considered Addendum A to this SPP. This Plan shall be posted in Sec-Con and will be considered a living document.

27. Addendum B - Safeguarding of Classified Materials

The Safeguarding of Classified Materials Plan is considered Addendum B to this SPP. This Plan shall be posted in Sec-Con and will be considered a living document.