Industrial Security Standard Practices and Procedures (SPP)

PeopleReady, Inc.

1015 A Street
Tacoma, WA 957 7

Forward

PeopleReady, Inc. has entered into a Security Agreement with the Department of Defense 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) or 32 CFR NISPOM RULE. 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 32 CFR NISPOM RULE is available for review by contacting the Facility Security Officer.

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.

As of the date of this manual, PeopleReady, Inc., is not authorized to safeguard classified material at its corporate facilities. We may not access, open, read, or store classified material in our company spaces.

Brittany Taylor 06/08/2022

Brittany Taylor Date
Facility Security Officer

DocuSigned by:
Taryn Owen 8/2/2022
FFB4BDF9DF91467...

Taryn Owen Date
President

Table of Contents

1. Introduction

This Standard Practices and Procedures (SPP) describes PeopleReady, Inc. 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 NISPOM RULE), which takes precedence in instances of apparent conflict.

2. Facility Information

2.1. Facility Clearance

A facility clearance (FCL) is an administrative determination that, from a security viewpoint, a company is eligible for access to classified information or award of a classified contract. PeopleReady, Inc. has a Secret facility clearance. The FCL is valid for access to classified information at the Secret or lower classification level.

2.2. Facility Security Officer

Having a facility clearance PeopleReady, Inc. must agree to adhere to the rules of the National Industrial Security Program (NISP). As part of the NISP, contractors are responsible for appointing a Facility Security Officer (FSO). The FSO must be a U.S. citizen, an employee of the company, and cleared to the level of the facility clearance. The FSO must complete required training and is responsible for supervising and directing security measures necessary for implementing the NISPOM and related Federal requirements for classified information.

Brittany Taylor is the FSO for PeopleReady, Inc. and can be reached at 425-971-5852 or bforshee@peopleready.com

2.3. Senior Management Official

The Senior Management Official (SMO) is the contractor's official responsible for the entity policy and Strategy. The SMO is an entity employee occupying a senior position in the entity with ultimate authority over the facility's operation and the authority to direct actions necessary for safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or locations. The SMO should be cleared at the same level of the facility clearance.

Pursuant to 32 CFR 117.7 (b)(2), the SMO will:

- Ensure our company maintains a system of security controls in accordance with the requirement of 32 CFR Part 117, NISPOM.
- Appoint a contractor employee or employees, in writing as the FSO and ITPSO
- Remain fully informed of the facility's classified operations.
- Make decisions based on classified threats reporting and their thorough knowledge, understanding, and appreciation of threat information and the potential impacts cause by the loss of classified operations.

- Retain accountability for the management and operations of the facility without delegating that accountability to a subordinate manager.

Taryn Owen is the SMO for our company and can be reached at towen@peopleready.com, or 913-709-2494.

2.4. Insider Threat Program Senior Official

Our Company SMO has appointed the ITPSO who should be cleared to the same level as the facility clearance. The ITPSO will complete training pursuant to 32 CFR 117.12 to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, and consistent with E.O.13587 and Presidential Memorandum "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs." See our Company Insider Threat Plan.

Brittany Taylor is the ITPSO for our company and can be reached at bforshee@peopleready.com or 757- 230-2866

Our company has established and will maintain an insider threat program in accordance with 32 CFR 117.7 (c).

2.5. Information System Security Manager

Currently, PeopleReady, Inc. is not processing classified information on an information system located at our facility and does not have an ISSM appointed. Once an ISSM is appointed PeopleReady, Inc. will notify DCSA if there is a change.

Prior to requesting an approval to process classified information at our facility, PeopleReady, Inc. will appoint an ISSM who is eligible for access to classified information to the highest level of the information processed on the system(s) under their responsibility. The ISSM will oversee development, implementation, and evaluation of their contractor's classified information system program.

PeopleReady, Inc. will ensure that the ISSM is adequately trained and possess technical competence commensurate with the complexity of the contractor's classified information system. ISSM responsibilities are specified in 32 CFR 117.18, if applicable.

2.6. Storage Capability

The facility clearance level is separate from the storage capability level. Contractors must receive a separate approval prior to storing any classified information. **PeopleReady, Inc. has NOT been approved to store classified material.** Section 9 discusses the procedures for appropriate handling, storage, and control of classified materials within our facility if we had the requirement to do so.

2.7. Cooperation with Federal Agencies

Our company will cooperate with Federal agencies and their officially credentialed USG or contractor representatives during, at a minimum:

- Official reviews.
- Investigations concerning the protection of a classified information.

- Personnel security investigations of present or former employees and others (e.g., consultants or visitors).

Cooperation includes:

- Providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours.
- Providing, when requested, relevant employment, personnel files, security records, supervisory records, records pertinent to insider threat (e.g., security, cybersecurity, and human resources) and any other records pertaining to an individual under investigation that are, in the possession or control of PeopleReady, Inc. or its representative or located in in its office.
- Provide access to employment and security records that are located at an offsite location, as applicable.
- Rendering other assistance, if necessary.

Questions related to an Agent's/Investigator's identity or status should be directed to DCSA Physical Security: 1-888-795-5673 or RMFSIMSST@nbib.gov

3. Personnel Security Clearances 32 CFR 117.10

3.1. Clearance Procedures

PeopleReady, Inc. employees will be processed for a personnel security clearance (PCL) only when a determination has been made that access is necessary for performance on a classified contract. The number of employees processed for a clearance will be limited to the minimum necessary for operation efficiency.

PeopleReady, Inc. will utilize the Defense Information System for Security (DISS) to initiate the clearance request process. Each applicant for a security clearance must produce evidence of citizenship such as an original birth certificate or passport. Applicants will complete the Questionnaire for National Security Positions (SF-86) through OPM's electronic questionnaires for investigation processing (e-QIP) system.

The FSO will ensure that prior to initiating the e-QIP action, the applicant is provided a copy of 32 CFR NISPOM RULE 117.10 (d)(1)(2). This ensures the employee is aware that the SF-86 is subject to review by the FSO only to determine the information is adequate and complete but will be used for no other purpose and protected in accordance with the Privacy Act of 1975.

3.2. Commitment for Employment – 32 CFR 117.10 (f)(1)(i)(ii)(f)(2)(3)

While PeopleReady, Inc. initiates the clearance process for employees, the government will make the determination of whether or not an individual is eligible to access classified information and grant the personnel clearance.

3.3. Investigative Tiers and Processes

There are three investigative tiers:

- Tier 1 is for positions designated as low risk, non-sensitive and allows physical and/or logical access to government facilities and computer systems

- Tier 3 is for positions designated as moderate risk, non-critical sensitive and allow access to information classified at the L, CONFIDENTIAL, and SECRET levels.
- Tier 5 is for positions designated as high risk, critical sensitive, special sensitive and allow access to information classified at the Q, TOP SECRET, and SCI level.

Investigators will use a variety of resources and methods to collect, verify, corroborate, or discover information about an individual, as documented on the request for investigation or developed from another source, including:

- Automated sources such as automated record checks and inquiries.
- Interview, if required, will cover areas of adjudicative concern.
- Information validated in a prior investigation, the results of which are not expected to change (i.e., verification of education, degree) will not be repeated as part of subsequent investigations.
- Polygraph examinations for agencies with policies authorizing the use of the polygraph for purposes of determining eligibility for access to classified information.
- Financial disclosure forms may be required by specific Government Contracting Activity (GCA).

3.4. Reinvestigations

DoD has implemented an ongoing screening process to review the background of an individual who is assigned to a sensitive position or has access to classified information or material. This "continuous vetting" process will eventually replace the requirement for Period Reinvestigation (PR)'s.

Depending upon the level of access required, individuals holding security clearances are subject to a periodic reinvestigation (PR) at a minimum of every six years for Top Secret, 10 years for Secret and 15 years for Confidential. Our FSO is responsible for reviewing all access records to ensure employees are submitted for PRs as required.

PR's will now be calculated by reviewing both the date of the last completed investigation and the Continuous Evaluation enrollment reason and date.

- If the individual shows a continuous evaluation (CE) enrollment reason of CE deferred, the next PR should be submitted based on the CE deferred date.
- If the individual shows a continuous evaluation enrollment reason of CE adjudication deferred, the next PR should be submitted based on the CE adjudication deferred date.
- If the individual shows continuous evaluation enrollment reason of CE other, the next pr should be submitted based on the last completed investigation date.

3.5. Consultants - 32 CFR 117.10 (m)

For security administration purposes, consultants are treated as employees of PeopleReady, Inc. and must comply with this SPP and the CFR NISPOM RULE. Consultants will, however, be required to execute a Consultant Agreement which outlines any security responsibilities specific to the consultant.

Note: If PeopleReady, Inc. sponsors a consultant for a PCL, PeopleReady, Inc. must compensate the consultant directly; otherwise, the company receiving compensation must obtain a Facility Security Clearance (FCL) and serve as a subcontractor to PeopleReady, Inc.

3.6. Pre-Employment PCL Determination Actions

Per 32 CFR 117.10 (f), is a potential employee requires access to classified information immediately upon commencement of employment, PeopleReady, Inc. may submit a request for investigation prior to the date of employment, provided:

- A written commitment for employment has been made by PeopleReady, Inc.
- The candidate has accepted the offer in writing.

3.7. Pre-Employment PCL Determination Actions

The commitment for employment must indicate employment will commence within 45 days of the employee being granted eligibility for access to classified information at a level that allows them to perform the tasks or services associated with the contract requirement for which they were hired.

3.8. SF312 and other NDA

Per 32 CFR 117.10 (g), the Standard Form 312 is a nondisclosure agreement between the USG and an individual who is determined eligible for access to classified information. Other CSAs have additional sensitive compartmented information NDA's (e.g., Form 4414).

Employees determined eligible for access to classified information must execute the NDA (s) prior to being granted access to classified information. Employee must sign and date the NDA(s) in the presence of a witness. The employee's and witness signatures must bear the same date. The FSO uploads the executed SF 312 into DISS for retention prior to granting the employee access to classified information. If an employee refuses to execute the NDA (s), PeopleReady, Inc. will deny the employee access to classified information and submit a report to the CSA in accordance with 32 CFR 117.18 (c)(6).

3.9. PCL Reciprocity

32 CFR 117.10 (h), DCSA or the applicable CSA determines whether contractor employees have been previously determined eligible for access to classified information or investigated by an authorized investigative activity in accordance with SEAD 7.

4. Individual and Corporate Reporting Responsibilities 32 CFR 117.18 (c) (1)(ii)

4.1. Adverse Information - 32 CFR 117.18 (c)(1)(i)(ii)

Adverse Information is any information regarding a cleared employee or employee in process for a security clearance which suggests that his/her ability to safeguard classified information may be impaired or that his or her access to classified information may not be in the interest of national security. Cleared personnel must report to the FSO, any adverse or information regarding himself, herself, or another cleared individual to the FSO. Reportable adverse information includes:

- Relationships with any known saboteur, spy, traitor, anarchist, or any espionage or secret agent of a foreign nation.

- Serious mental instability or treatment of any mental institution.
- Use of illegal substances or excessive use of alcohol or other prescription drugs.
- 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 of 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.

The FSO will report this information immediately to the DCSA Vetting Risk Operations (VRO) office via the incident report function in DISS.

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. Foreign Travel

All cleared employees or employees who are in a position that is considered sensitive in nature, must now report foreign travel at least 30 days in advance. This information will be tracked in DISS by DCSA. In your initial email to the FSO or designee the following information will be required:

- Date of travel:
- Countries to be visited:
- Names of Non-US Citizens as well as their citizenship, that you plan to see while out of the country:
- Method travel used:

You will then receive an email that will contain pertinent information on the country(s) that you are visiting.

Foreign travel emails should be emailed to bforshee@peopleready.com.

Upon your return you will need to call or see the FSO or designee and let them know if any of the items listed below happened during your foreign travel:

- Did your dates of travel change?
- Did you go to any other countries other than the ones that you reported before you left?
- Names of any additional Non-US Citizen(s), if applicable.
- Where you asked any questions of a suspicious nature?
- Did anyone seem overly curious regarding your job or company?
- Did you apply for citizenship?
- Did you open an account for a foreign bank?
- Did you purchase foreign property(s)?

If you live near the borders of Mexico or Canada and take a day trip to either country, this needs to be reported within 5 days of your return to work to the FSO or designee.

5. Security Education 32 CFR 117.12

5.1. Insider Threat Training

The PeopleReady, Inc. Insider Threat Program Senior Official (ITPSO) Brittany Taylor ensures assigned insider threat program personnel and all cleared employees complete training consistent with applicable CSA provided guidance. See PeopleReady, Inc. Insider Threat Program's Insider Threat Training section for specific personnel functional or role requirements

PeopleReady, Inc. employees must complete insider threat awareness training annually. All newly cleared employees complete training before granted access to classified information.

Insider Threat awareness training covers current and potential threats in the workplace and personal environment and will include at a minimum:

- The importance of detecting potential insider threats by cleared employees and reporting suspected activities to the insider threat program designee.
- Methodologies of adversaries to recruit trusted insider and collect classified information in particular within information systems.
- Indicators of insider threat behavior and procedures to report such behavior.
- Counterintelligence (CI) and security reporting requirement, as applicable.

5.2. Initial Security Briefing

All cleared employees must receive an initial security briefing and sign a Nondisclosure Agreement (SF 312) prior to being granted access to classified material. The SF312 only needs to be signed if one is not uploaded into DISS. 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, including Insider Threat awareness.
- Counterintelligence Awareness.
- Overview of Security Classification System.
- Employee reporting obligations and requirements, including insider threat.
- Cybersecurity training for all authorized information systems users.
- Security procedures and duties applicable to the employee's position requirements (e.g., marking and safeguarding of classified information).
- Criminal, civil, or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not yet signed an NDA.
- Insider Threat Training.
- CUI training. While outside the requirements of the NISPOM, when a classified contract includes provisions for CUI training, contractors will comply with those contract requirements.
- Overview of the SPP.

5.3. Annual Security – 32 CFR 117.12 (k)

Annual briefings will be provided to all cleared employees and employees who are in a position that is considered sensitive in nature, to remind employees of their obligation to protect sensitive or classified information, as well as to provide any updates to security requirements.

5.4. Debriefings - 32 CFR 117.12 (l)

When a cleared employee no longer requires a security clearance or terminates employment with PeopleReady, Inc., the employee will be debriefed by the FSO, and access will be immediately removed from DISS.

5.5. Derivative Classification Training - 32 CFR 117.12 (h) (1) & (2)

PeopleReady, Inc. employees who have been authorized to make derivative classification decisions must complete initial derivative classification training and refresher training at least once every 2 years before being authorized to make derivative classification decisions. Documentation will be retained identifying the date of the most recent training and type of training derivative classifiers receive. Contact the FSO for guidance on how to access and complete the training.

6. Security Reviews/Self-Inspections

6.1. Defense Counterintelligence and Security Agency

The 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) of the facility, an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance to you and PeopleReady, Inc. on security related issues.

Our assigned DCSA field office is:

NAESOC Field Office
Defense Counterintelligence and Security Agency (DCSA)
P.O. Box 644
Hanover, MD 21076

6.2. Security Reviews (SR)

PeopleReady, Inc. will be assessed by the DCSA on a bi-annual cycle. During this time, DCSA Industrial Security Representatives will review our security processes and procedures to ensure compliance with the 32 CFR NISPOM RULE, and interview PeopleReady, Inc. employees to assess the effectiveness of the security program. Your cooperation with DCSA during the SR is required.

6.3. Self-Inspections - 32 CFR 117.17(g)(2)

PeopleReady, Inc. FSO or designee will also perform a self-inspection, similar to the DCSA SR. This self-inspection should be done at least once annually but no more than 365 calendar days apart.

The purpose is to self-assess the security procedures to determine the effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, PeopleReady, Inc. employees will be interviewed. The results of the self-inspection will be briefed to employees during refresher briefings.

The FSO is also required to prepare a formal report describing the self-inspection, its findings and its resolution of issues discovered during the self-inspection. This formal report should be signed by the SMO and uploaded in NISS.

7. Individual & Corporate Reporting Responsibilities 32 CFR 117.8

All PeopleReady, Inc. employees are to immediately report any of the following information to the FSO. Our FSO Brittany Taylor can be reached at rbforshee@peopleready.com, 757- 230-2866. Reports can be made verbally, via mail, or via telephone but if made verbally or via telephone, should always follow up with an email notification.

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

7.1. Espionage/Sabotage - 32 CFR 17.18 (a)(2)(iii)

Employees should report to the FSO immediately any information concerning existing or threatened espionage, sabotage, or subversive activities. Examples of these types of reports include:

- Handing over information that would either interfere with the US military or promote the success of the country's enemies.
- Attempting to interfere with military operations or promoting the success of the country's enemies by communicating false statements during wartime.
- Destroying or damaging harbor-defense property.
- Destroying or damaging war material, premises, or utilities.
- Producing defective national defense material, premises, or utilities.

If the employee is unable to contact the FSO in a timely manner, they should report directly to the FBI and follow-up with their FSO.

7.2. Suspicious Contacts 32 CFR 117.18 (c)(2)

Suspicious contacts are efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise cleared employees.

Examples of suspicious contacts include:

- Receipt of a foreign national resume where the job advertisement states that a clearance is required.
- Request for protected information under the guise of a price quote or purchase request, market survey, or another pretense.

- Foreign entities targeting cleared employees traveling overseas via airport screening or hotel room incursions.
- Attempts to entice cleared employees into situations that could lead to blackmail or extortion.
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file.
- Attempts to place cleared personnel under obligations through special treatment, favors, gifts or money.
- Former cleared or trusted employees attempting to gather controlled or classified information from previous co-workers.

Employees should report all suspicious contacts to the FSO.

The FSO will forward all reports to the respective government agency for review and action with a courtesy copy to their DCSA ISR.

7.3. Adverse Information - 117-18 (c)(1)(i)(ii)

Adverse information is any information regarding a cleared employee or employee in process for a clearance which suggests that his/her ability to safeguard classified information may be impaired or that his or her access to classified information may not be in the interest of national security. Cleared personnel report adverse information regarding themselves, or another cleared individual to the FSO. Reportable adverse information may include:

- 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 other prescription drugs.
- Excessive debt, including garnishments on 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 U.S. Government by unconstitutional means.
- Involvement in the theft of, or any damage to, Government property.

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

7.4. Loss, Compromise, or Suspected Compromise of Classified Information - CFR 117.18 (d)

Cleared personnel must immediately report the loss, compromise, or suspected compromise of classified information.

The FSO will report this information immediately to their DCSA ISR. The report should be made initially via email.

7.5. Individual Culpability Reports/Security Violations

Cleared personnel must immediately report to the FSO any failure to comply with a requirement of this SPP or of the 32 CFR NISPOM RULE. See Section 8 regarding PeopleReady, Inc. graduated scale of disciplinary actions.

Examples of culpability reports include:

- Deliberate disregard of security requirements.
- Gross negligence in the handling of classified material.
- A pattern of negligence or carelessness.

The FSO will report this information immediately to the DCSA VRO office via the incident report function in DISS.

7.6. FCL Changes

Per 32 CFR 117.8 (c)(7), company leadership must report facility changes to the FSO which include:

- Change of ownership or control, including stock transfers that affect control of the entity.
- Change of operating name or address of any of its locations determined eligible for access to classified information.
- Any change to the information previously submitted for KMP's.
- Any action to terminate business or operations for any reason imminent adjudication or reorganization in bankruptcy, or any changes that might affect the validity of the eligibility for access to classified information.
- Any Material change concerning the information previously reported concerning foreign ownership, control, or influence (FOCI).

The FSO will report this information immediately to their DCSA ISR via email.

7.7. Cleared Personnel Changes

Cleared personnel must immediately report to the FSO personal changes to include:

- Change in name.
- Death.
- 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 or perform classified work.
- Refusal by an employee to sign the SF312, "Classified Information Nondisclosure Agreement".
- Citizenship by naturalization for the non-US citizens granted a Limited Access Authorization.

The FSO will report this information immediately to the DCSA VRO office via the CSR function in DISS.

7.8. Cleared Personal Changes Unsatisfactory Conditions of a Prime or Subcontractors

Per 32 CFR 117.8 (c)(10), and (c)(14), with respect to the responsibilities for reporting to be submitted to the DCSA, each subcontractor will be considered as a prime contractor in relation to its own employees or subcontractor(s). Subcontractors will also notify the prime contractors if they make any reports to DCSA related to FCL changes, changes in storage capacity and inability to safeguard classified information.

Prime contractors will report any information coming to their attention that may indicate that classified information cannot be adequately protected by a subcontractor, or other circumstances that may impact the validity of the eligibility for access to classified information of any subcontractor.

Subcontractors will report any information coming to their attention that may indicate that classified information cannot be adequately protected for other circumstances that may impact the validly of the eligibility for access to classified information by their prime contractor.

The employee will report to their FSO any of the above conditions.

The FSO will report this information immediately to their DCSA ISR.

7.9. Security Equipment Vulnerabilities, Change in Storage Capacity, Ability to Safeguard Classified Material, and Dispositioned Material Previously Terminated

Personnel must immediately report significant vulnerability in security equipment or hardware/software that could possibly lead to the loss or compromise of classified information.

The FSO will report this information immediately to their DCSA ISR via email.

7.10. Foreign Classified Contracts

Per 32 CFR 117.8 (c)(12), and (c)(13), we must report any pre-contract negotiation or award not placed through DCSA or USG contracting activities that involves or may involve the release of disclosure of U.S. classified information to a foreign interest or access to classified information furnished by a foreign interest.

We must report to DCSA the receipt of classified material from foreign interests that is not received through Government channels.

The employee will report to their FSO any of the above conditions.

The FSO will report this information immediately to their DCSA ISR.

7.11. Reports to Information Security Oversight office (ISOO)

Per 32 CFR 117.8 (g) PeopleReady, Inc. must report to the Director of Information Security Oversight o\Office (ISOO), National Archives and Records Administration, instances of redundant or duplicative security review and audit activity by DCSAs for resolution. If there is an existing determination of an entity's eligibility for access to classified information and another CSA is required duplicating processing to determine an entity's eligibility for access to classified information, PeopleReady, Inc. will these report these instances to ISOO.

The employee will report to the FSO any of the above conditions.

The FSO will report this information immediately to the ISOO. You can begin by calling 1-86-NARA-NARA or (1-866-272-6272).

8. Graduated Scale of Disciplinary Actions

8.1. Graduated Scale

PeopleReady, Inc. will use the following graduated scale of disciplinary actions as a guide in determining appropriate administrative actions to assign to security violations:

Violations could result in the following disciplinary actions:

- Verbal counseling.
- Written counseling.
- Employment suspension or termination.

8.2. Major Offenses

For security violations involving a deliberate disregard of the SPP and 32 CFR 117, NISPOM requirements or when an employee exhibits a pattern of questionable judgement, irresponsibility's, negligence, or carelessness, the FSO has the authority to recommend through the DISS system with information about the security violation, which may result in loss of the security clearance.

8.3. Minor Offenses – First Offense

In cases that are not deliberate and may be accidental or inadvertent, the FSO will meet with the employee to determine the severity of the security violation. The FSO will provide the employee with additional training and education to reduce the possibility of a similar incident happening again. The FSO will discuss the severity of the offense with the employee. The FSO will issue a verbal reprimand but will not file a report to the employee's PeopleReady, Inc. security file.

8.4. Minor Offenses – Second Offense

The FSO will meet with the employee to determine the cause of the security violation. The FSO will provide the employee with additional training and education to reduce the possibility of a similar incident happening again. The FSO will place a written reprimand in the PeopleReady, Inc. security file for a period of one year. The FSO will warn the employee that additional offenses may result in loss of security clearance, removal from project, unpaid leave and/or termination of employment.

8.5. Multiple Offenses

Multiple offenses are deemed to be blatant disregard for the SPP and 32 CFR 117, NISPOM requirements. The FSO may request the employee be removed from classified project work. The FSO may also recommend to management that the employee get a reduction in salary or that the employee's employment be terminated if work cannot be found for the employee that

does not require a security clearance. The FSO will submit an individual culpability report in DISS. Once the FSO reports the offices USG, DCSA or the USG contracting activity may decide to temporarily suspend or permanently remove the individual's security clearance depending on the seriousness of the violations.

9. Defense Hotline 117.7 (i)

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 Department of Defense, 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.

DEFENSE HOTLINE

TELEPHONE: 800-424-9098
http://www.dodig.mil/hotline

10. Controlled Unclassified Information (CUI)

10.1. CUI

Controlled Unclassified Information (CUI) is unclassified information requiring safeguarding and dissemination controls, consistent with applicable laws, regulations, or government-wide policy. There are two designations for CUI – Basic and Specific

CUI Basic is the subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls.

CUI Specified is the subset of CUI in which the authorizing law, regulation, or government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic.

The distinction is the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic Information.

10.2. CUI Manager

PeopleReady, Inc. has appointed a CUI Manager to manage the facility's CUI Program. The CUI manager is a US Citizen and has completed initial CUI Training.

The CUI Manager will complete/has completed required training when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements and is responsible for developing and implementing security guidance necessary for CUI program implementation. Training is required annually for Department of Defense (DOD) contracts and bi-annually for non-DOD contracts.

Brittany Taylor is the CUI Manager for PeopleReady, Inc. and ca be reached at bforshee@peopleready.com or 757-230-2866

10.3. CUI Training and Awareness

Initial Training

- All employees that handle CUI as part of their duties should complete required training when requested by the Government Contracting Activity (GCA) for contracts with CUI requirements.
- Per DoDI 5200.48, DOD contractors require initial training and annual refresher training on CUI.
- Industry should note that this requirement is different from agencies governed by 32 CFR 2002, which requires refresher training every 2 years
- The Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) provides CUI training that is available to industry (IF141.06). The course fulfills CUI training requirements for industry when it is required by Government Contracting Activities for contracts with CUI requirements (and for all employees that handle CUI as part of their duties)

10.4. CUI Annual Refresher Training

PeopleReady, Inc. will provide annual refresher training to all employees handling CUI in order to remind employees of their obligation to protect CUI and provide any updates to security requirements.

10.5. CUI Training Records

The CUI Manager will maintain records showing names of employees who have taken the initial, refresher training, the method of the course delivery and the date of completion.

10.6. CUI Self Inspection

The CUI Manager will review the CUI Self-Inspection Appendix to assist in the initial establishment of PeopleReady, Inc. CUI Program. Once established, the CUI Self-Inspections Appendix should be considered to self-assess the CUI Security procedures determine compliance and effectives of PeopleReady, Inc. CUI Program and identify and deficiencies/weakness. The self-inspection results must be documented. The results of the self-inspection will be briefed to employees during refresher training.

10.7. CUI Lifecycles

CUI follows a life cycle similar to all protected information. While the design of certain types of information requiring safeguard and dissemination may be new, the process should be very familiar.

10.8. CUI Unauthorized Disclosure and CUI Misuse

Unauthorized Disclosure (UD)

- UD is when CUI is disclosed to someone without a lawful government purpose or to someone incapable of providing adequate security over the CUI. A UD is described as communications or physical transfer of classified or CUI to an unauthorized recipient. The CUI Manager must report UD of CUI to the DCSA ESO Office mailbox at dcsa.quantico.ctp.mbx.eso-unauthorized-disclosure@mail.mil.

CUI Misuse

- Misuse of CUI is an occurrence that takes place when someone use CUI in a manner not in accordance with the policy contained in the E.O. 13556, CFR 2002, the CUI Registry, agency CUI policy, or the applicable laws, regulations and Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.
- When a CUI misuse occurs, the CUI Manger is responsible for conducting a preliminary Administrative Inquiry (AI). The purpose of the preliminary inquiry is to secure the CUI information quickly and gather the available facts and determine if the CUI information was subject to compromise. If the CUI Manager concludes, based on the preliminary AI, that no loss, compromised or suspected compromise, or suspected compromise occurred, the CUI Manager has the responsibility to finalize the inquiry.

10.9. CUI Handling Responsibilities for Information Owners & End Users

All PeopleReady, Inc. employees are responsible for the content they create or send over company email, Internet, or text.

- All CUI must be access-controlled for authorization and limited to individuals who possess a lawful government purpose to access the information.
- CUI must only be transferred to locations, persons, and entities that meet the requirements to provide adequate security for CUI.
- All CUI digitally sent must be encrypted using authorized tools and/or solutions.
- CUI must never be accessed from, processed on, transmitted from, or stored on public computer (i.e., internet kiosks, airports, hotel business centers, etc.).
- When working with CUI it Is required to establish a controlled environment that will safeguard CUI. Therefore, to access or store CUI in an authorized mobile phone or tablet, the device must adhere to CUI safeguarding contractual requirements.
- CUI must not be sent via text message capabilities (SMS).
- CUI must not be captured via personal camera from any source (e.g., whiteboard).

10.10. Compliance and Acknowledgement

Employees of PeopleReady, Inc. understand the end-user responsibilities to identify, handle, process, and protect CUI in the performance of their duties and in performance of a government contract and that non-compliance with the standards may result in disciplinary measures up to and including termination of employment.

Employees of PeopleReady, Inc. should contact the CUI Manager if there are any questions about any of the sections in this document.

11. Marking Classified Information

11.1. 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.
- ***CUI –*** Material that if compromised could cause damage to national security or release information that shouldn't be in everyone's hands.

11.2. Original Classification

The determination to originally classify information may be made ONLY by a U.S. 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.

11.3. Derivative Classification

PeopleReady, Inc. employees authorized to perform derivative classification actions must have adequate training and the proper classification guides and/or guidance necessary to accomplish these important actions. See Section 4.4 regarding required derivative classification training.

12. Safeguarding Classified Information 32 CFR 117.15

12.1. 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.

12.2. Oral Discussions

PeopleReady, Inc. employees shall 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 FSO to determine which areas have been designated for classified discussions.

12.3. End-of-Day Checks – 117.15 (a) (2)

To ensure that all storage containers are properly secured, the following procedures will be followed at the end of each business day:

NOTE: Classified information cannot be stored, reproduced, received at PeopleReady, Inc. as PeopleReady, Inc. is not approved for classified storage. If PeopleReady, Inc. becomes approved, we will follow section 10.

12.4. Perimeter Controls

If PeopleReady, Inc. was authorized to store classified, we would have perimeter controls established at PeopleReady, Inc. to deter and detect unauthorized introduction or removal of classified material. There is a sign conspicuously posted at the front and rear entrances stating that all persons who enter or exit the facility shall be subject to an inspection of their personal effects. All visitors and employees are subject to possible inspection, which will occur at random intervals.

12.5. Receiving Classified Material

PeopleReady, Inc. is not approved to receive classified email.

12.6. Storage of Classified Information

PeopleReady, Inc. is currently not approved to store classified.

Only a minimum number of authorized individuals will have knowledge of the combinations for security containers where classified material is stored. The following procedures apply:

- A record of individuals with access to each container is maintained.
- Containers must be locked when not under direct supervision of an authorized individual.
- All classified material must be secured in the appropriate security container at the end of each working day.

NOTE: Classified information cannot be removed or stored at PeopleReady, Inc. for use or storage at an individual's private residence.

12.7. Combinations

PeopleReady, Inc. is not authorized to store classified. If PeopleReady, Inc. had authorized, designated employees should memorize the combinations of classified security containers. If a written record of the combination is established, it will be marked and safeguarded in accordance with the highest level of material stored in the container.

Combinations will be changed as soon as possible following:

- The initial receipt of an approved container or lock.
- The reassignment, transfer, termination of any person having knowledge of the combination, or when the security clearance granted to any such person is downgraded to a level lower than the category of material stored, or when the clearance has been administratively terminated, suspended, or revoked.

- The compromise or suspected compromise of a container or its combination, or the discovery of a container left unlocked or unattended.

The combination will be changed by a person authorized access to the contents of the container or by the FSO.

12.8. Transmission of Classified Information

PeopleReady, Inc. is not authorized to transmit classified.

12.9. Reproduction of Classified Material

PeopleReady, Inc. is not authorized to reproduce classified.

12.10. Destruction of Classified Material

PeopleReady, Inc. is not authorized to destroy classified.

12.11. Retention of Classified Materials

PeopleReady, Inc. is not authorized to store classified.

13. Public Release/Disclosure

13.1. Disclosure

PeopleReady, Inc. 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 see the FSO to determine if we must obtain approval from the customer.

Note: Classified information made public is not automatically considered unclassified. PeopleReady, Inc. shall continue the classification until formally advised to the contrary.

13.2. Disclosure to Subcontractors and Other Contractors

Per 32 CFR 117.15 (h)(2) PeopleReady, Inc. may only disclose classified information to a cleared subcontractor with the appropriate entity eligibility and need to know when access to classified information is necessary for the performance of tasks or services essential to the fulfillment of a prime contract or a subcontract.

PeopleReady, Inc. will convey appropriate classification guidance for the classified information to be disclosed with the subcontractor in accordance with Per 32 CFR 117.13.

PeopleReady, Inc. may only disclose classified information to the subcontractor id DCSA (or other applicable CSA) has already:

- Pre-determine the subcontractor to be eligible for access to classified information at the same level or higher than the classified information to be disclosed.

- Approved storage capability for classified material at the subcontractor location if a physical transfer of classified material is to occur.

Per 32 CFR 117.15 (h)(6) PeopleReady, Inc. may not disclose any classified information to another contractor except in furtherance of a contract, subcontract or other GCA purpose without the authorization of the GCA if such authorization if required by contract.

PeopleReady, Inc. is not authorized to store classified information.

13.3. Disclosure to Federal Agencies

Per 32 CFR 117.15 (h)(4) PeopleReady, Inc. may not disclose any classified information received or generated under a contract from one agency to any other federal agency unless specifically authorized by the agency that has classification jurisdiction over the information.

13.4. Disclosure to Foreign Persons

Per 32 CFR 117.15 (h)(5), PeopleReady, Inc. may not disclose any classified information to foreign persons unless specified by the contract and release of the information is authorized in writing by the government agency having classification jurisdiction over the information involved, i.e., the DOE for Restricted Data (RD) and Formally Restricted Data (FRD) (also see Per 32 CFR 117.23), the NSA for COMSEC, the DNI for SCI, and all other executive branch departments and agencies for classified information under their respective jurisdictions.

13.5. Disclosure to Connection with Litigation

Per 32 CFR 117.15 (h)(7) PeopleReady, Inc. may NOT disclose classified information to:

- Attorneys hired solely to represent PeopleReady, Inc. in any civil or criminal case in federal or state courts unless the disclose is specifically authorized by the agency that has jurisdiction over the information.
- Any federal or state court except on specific instructions of the agency, which has jurisdiction over the information or the attorney representing the United States in the case.

13.6. Public Release

Per 32 CFR 117.15 (h)(8) PeopleReady, Inc. may NOT disclosure classified information to the public. Contact the FSO to determine the process for obtaining prior GCA approval.

PeopleReady, Inc. may not disclose unclassified information pertaining to a classified contract to the public without prior review and clearance as specific in the Contract Security Classification Specification, or equivalent, for the contract or as otherwise specified by the GCA. The procedures of this paragraph also apply to information pertaining to classified contracts intended for use in unclassified brochures, promotional sales literature, reports to stockholders, or similar material. Furthermore, this requirement applies to any information developed subsequent to the initial approval through the appropriate office prior to public disclosure.

However, unless restricted by an applicable CSA by contract requirements PeopleReady, Inc. does not need to request approval for disclosure of:

- The fact that a contract has been received, including the subject matter of the contract or type of item in general terms provided the name or description of the subject matter is not classified.
- The method or type of contract.
- Total dollar amount of the contract unless that information equates to a level of effort in a sensitive research area and/or quantities of stocks of certain weapons and equipment that are classified.
- Whether the contract will require the firing or termination of employees.
- Other information that from time-to-time may be authorized on a case-by-case basis in a specific agreement.
- Information previously officially approved for public disclosure.

PeopleReady, Inc. may not disclose information that has been declassified if the information is comingled with CUI or qualifies as CUI once declassified. In such instances, PeopleReady, Inc. will mark and protect it as CUI until it is reviewed for public release or decontrolled pursuant to 32CFR part 2002. If the information does not qualify as CUI, it will be protected in accordance with the basic safeguarding requirements in 48 CFR 52.204-21 and subject to the GCA's public release procedures.

13.7. Improperly Released Classified Information

Per 32 CFR 117.13 (f), improperly released classified information is not automatically declassified. When classified information has been improperly released, and even when that classified information has become publicly available, PeopleReady, Inc. will:

- Continue to protect the information at the appropriate classification level until formally advised to the contrary by the GCA.
- Bring any questions about the propriety of continued classification in these cases to the immediate attention of the GCA.
- Notify DCSA if an employee downloads the improperly released classified information to determine how to resolve a data spill.

14. Visit Procedures

14.1. Incoming Visits

Per 32 CFR 117.16 (a), "Visits" concerns a lawful and authorized USG purpose, where it is anticipated that classified information will be disclosed at a cleared contractor facility or a USG facility.

PeopleReady, Inc. does NOT currently have approval to safeguard classified materials at its facility. As such, there is no storage at the facility, and it is unlikely that there will be any classified visits at PeopleReady, Inc. location.

PeopleReady, Inc. will limit the number of classified visits to other cleared contractor or USG facilities to a minimum where a meeting is necessary and where the purpose of the visit cannot be achieved without access to or disclosure of classified information.

The FSO will ensure procedures are implemented for positive identification of visitors, verification of appropriate personnel clearances (via a visit authorization letter) and a need-to-know determination prior to the disclosure of any classified information at a level that is consistent with visit purposes for both incoming and outgoing visit.

The responsibility for determining need-to-know in connection with a classified visit request with the individual who will disclose classified information during the visit. 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 contractors has a bona fide need to access the information in furtherance of a GCA purpose. For visits to USG or other contractor facilities, (PeopleReady, Inc.) employee must notify the FSO and provide the contractor or agency to be visited, authorization letter requests preparation and submission via DISS to the contractor /agency and may not proceed with the visit until it is received/processed by the contractor/agency visitor control.

All incoming classified visits must be approved in advance of the visit by the FSO or designee The FSO is responsible for determining that the requesting contractor has been granted an appropriate facility clearance based upon an existing contractual relationship involving classified information of the same or higher classification category, or otherwise by verification through the DCSA web-based National Industrial Security System (NISS).

The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Prior to the disclosure of classified information to a visitor, positive identification of the person must be made.

14.2. Incoming Visits – Classified Visits by USG Representatives

Representatives of the USG, when acting in their official capacities as inspectors; investigators, or auditors, may visit PeopleReady, Inc. facility, provided these representative present appropriate USG credentials upon arrival.

14.3. Incoming Visits - Long-term Visitors

When employees of one contractor are temporarily stationed at another contractor's facility, the security procedures of the host contractor will govern.

PeopleReady, Inc. employees at USG installations will follow the security requirements of the host. This does not relieve PeopleReady, Inc. of its security oversight of PeopleReady, Inc. employees who are long-term visitors at USG installations.

14.4. Incoming Visits - Classified Visits

Per 32 CFR 117.16 (b), "Classified Meetings" concerns a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed. Disclosure of classified information to large diverse audiences such as conference increases security risk. Classified disclosure at such meetings may occur when it serves a government purpose and adequate security measures have been provided in advance.

PeopleReady, Inc. does NOT currently have security arrangements, authorized classified IT systems, and physical security in place that are necessary to be able to host classified

meetings. In the future if this changes, and if PeopleReady, Inc. plans to conduct classified meetings as a cleared contractor host, a USG agency must authorize the meeting and will security jurisdiction. Such meetings will comply with the security requirements in Per 32 CFR 117.16 (b).

PeopleReady, Inc. employees who need to attend a classified meeting must comply with cleared contractor host and/or USG agency requirements including possessing the requisite clearance and a need-to-know for the information to be disclosed. Contact the FSO for assistance in submitting the appropriate information for attending classified meetings with ample time for processing.

14.5. Incoming Visits – Visitor Log, Badging, IT Guest Access and Escorting

PeopleReady, Inc. maintains a visitor log for all cleared and uncleared visitors to the PeopleReady, Inc. facilities and has a badging process to distinguish visitors with varying level of access and whether they are foreign persons. PeopleReady, Inc. will not provide a keycard/FOB facility access to visitors.

The PeopleReady, Inc. employee visitor host or their designee will escort the visitors to the meeting in the PeopleReady, Inc., the visitor should not be left unattended and shall not move freely through the facility. However, when no meetings are taking place, the visitor may be left in one of the glass conference room a break if the escort/host has a visual line of sight on the visitor.

PeopleReady, Inc. will only grant visitors access to the guest IT network, which is separate from the PeopleReady, Inc. network. The guest IT network does not permit access to PeopleReady, Inc. information.

14.6. Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When it becomes necessary for employees of PeopleReady, Inc. 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, their SMO code, the time and duration of visit, the reason for the visit, and the name and phone number of the person to be contacted. Ample time should be allowed to permit the visit authorization request to be prepared, submitted via DISS to the contractor/agency, and processed by their visitor control.

15. Subcontracting

In the event that PeopleReady, Inc. decides to subcontract any work under a classified contract, it will comply with the security requirements of 32 CFR 117. The subcontractor must possess an appropriate entity eligibility determination and a classified information safeguarding capability if possession of classified information will be required. PeopleReady, Inc. will incorporate a “security requirements clause” and a “Contract Security Classification Specification,” or its equivalent in the subcontract. In most cases, subcontracting classified work will also require approval of the GCA. See the FSO for guidance on pre-and post-award security requirements related to subcontracting.

16. Information System Security – (Only for Approved Classified Systems)

The Information Systems Security Manager (ISSM) maintains System Security Plans (SSP) for all classified information systems. Refer to the SSPs for classified information systems requirements.

NOTE: Classified information CANNOT be entered into any computer or other electronic device at PeopleReady, Inc. as we have not been approved/accredited for classified processing. If you have any question as to whether a system is approved, please contact the FSO or ISSM.

17. Special Security Requirements

17.1. Design Information

PeopleReady, Inc. does not currently have special requirements for protection of Critical Nuclear Weapons Design Information (CNDWI). In the event that future contracts require this kind of access, PeopleReady, Inc. will implement procedures and comply with 32 CFR 117.20.

17.2. COMSEC

PeopleReady, Inc. does NOT currently have approval for classified COMSEC systems. In the event that future contracts require this kind of system. PeopleReady, Inc. will implement procedures and comply with 32 CFR 117.20.

17.3. DHS CCIP

PeopleReady, Inc. does NOT currently have approval for access to department of Homeland Security cybersecurity information sharing among critical infrastructure partners pursuant to E.O. 13691, In the event that future contracts require this kind of access PeopleReady, Inc. will implement procedures and comply with 32 CFR 117.22.

17.4. Other

PeopleReady, Inc. does NOT currently have any contract security requirements for:

- Critical Nuclear Weapons Design Information
- COMSEC
- DHS CCIPP
- Other
    - Alternative Compensatory Control Measure (ACCM}
    - Special Access Programs (SAP)
    - Sensitive Compartmented Information (SCI)
    - Restrictive Data (RD)
    - Formerly Restricted Data (FRD)
    - Trans-classified Foreign Nuclear Information (TFNI)
    - Naval Nuclear Propulsion Information (NNPI)
    - OPSEC

In the event that future contracts require this kind of access, PeopleReady, Inc. will implement procedures and comply with 32 CFR 117.23

18. Emergency Procedures 32 CFR 117.15 (a)(3)(iv)

18.1. Emergency Plan

In emergency situations, it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency situation 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.

***Also, Reference 117.8 (c)(9) - Inability to safeguard classified material. The contractor will report any emergency situation that renders their location incapable of safeguarding classified material as soon as possible.

19. 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.
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	All PeopleReady, Inc. 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 32 CFR 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.
Communication 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.
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 32 CFR NISPOM RULE 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 32 CFR 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 32 CFR NISPOM RULE.

20. Abbreviations & Acronyms

ACCM	Alternative Compensatory Control Measure
AFSO	Assistant Facility Security Officer
AIS	Automated Information System
C	Confidential
CAGE	Commercial and Government Entity
CDSE	Center for Development of Security Excellence
COMSEC	Communication Security
CNWDI	Critical Nuclear Weapons Design Information
CSA	Cognizant Security Agency
CSO	Cognizant Security Office
CUI	Controlled Unclassified Information
DoD	Department of Defense
DoD CAF	Department of Defense Central Adjudication Facility
DOE	Department of Energy
DCSA	Defense Counterintelligence and Security Agency
DTIC	Defense Technical Information Center
e-QIP	Electronic Questionnaire for Investigation Processing
FBI	Federal Bureau of Investigation
FCL	Facility Clearance Level
FRD	Formally Restricted Data
FSO	Facility Security Officer
GCA	Government Contracting Activity
GSA	General Services Administration
ISFD	Industrial Security Facilities Database
ISR	Industrial Security Representatives
ISSM	Information System Security Manager
ISOO	Information Security Oversite Office
ISSO	Information System Security Officer
ITPSO	Insider Threat Program Senior Official
ITAR	International Traffic in Arms
JPAS	Joint Personnel Adjudication System
KMP	Key Management Personnel
NNPI	Naval Nuclear Propulsion Information
NISP	National Industrial Security Program
NISS	National Industrial Security System
NISPOM	National Industrial Security Program Operating Manual
NTK	Need-To-Know
OPM	Office of Personnel Management
OPSEC	Operations Security
PCL	Personnel Security Clearance
POC	Point of Contact

PR	Periodic Reinvestigation
PSMO-I	Personnel Security Management Office for Industry
RD	Restrictive Data
S	Secret
SAP	Special Access Programs
SCG	Security Classification Guide
SF-312	Nondisclosure Agreement
SCi	Sensitive Compartmented Information
SMO	Senior Management Office
SPP	Standard Practice Procedures
SR	Security Review
TS	Top Secret
U	Unclassified
US	United States
USG	United States Government

21. References

- National Industrial Security Program Operating Manual (32 CFR 117 NISPOM Rule),
- DoDM 5220.32 Vol 1
- DoDM 5200.01 Vol 3Parts 2001 and 2003 Classified National Security Information; Final Rule
- SEAD 3
- SEAD 4
- SEAD 7
- Contractors Graduated Scale of Discipline.
- Contractor can provide other references as needed.