Logo, company name

Description automatically generated

STANDARD PRACTICE PROCEDURES (SPP)

E-volve Technology Systems

163 Waterfront Street Suite 420

Oxon Hill, MD 20745

Foreword

E-volve Technology Systems, Inc. has entered into a Security Agreement with the Department of Defense 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 conforms to the security requirements set forth in the government manual – the National Industrial Security Program Operating Manual or 32 CFR Part 117, the NISPOM Rule. The purpose of our SPP is to provide our employees with the requirements of the NISPOM Rule 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 Part 117, the NISPOM Rule is available for review by contacting the Facility Security Officer.

Our company fully supports the National Industrial Security Program. All of us have an obligation to ensure that our security practices contribute to the security of our nation’s classified defense information.

A picture containing text, blackboard, chain

Description automatically generated

Deidre J. Boone  
Senior Management Official

A picture containing text, chain, metalware

Description automatically generated

Tanya D. Johnson  
Facility Security Officer

Table of Contents

[1. Introduction 1](#_Toc143776906)

[2. Facility Information 1](#_Toc143776907)

[2.1. Facility Clearance 1](#_Toc143776908)

[2.2. Facility Security Officer 1](#_Toc143776909)

[2.3. Senior Management Official 1](#_Toc143776910)

[2.4. Insider Threat Program Senior Official 2](#_Toc143776911)

[2.5. Storage Capability 2](#_Toc143776912)

[2.6. Cooperation with Federal Agencies 2](#_Toc143776913)

[3. Personnel Security Clearances – §117.10 3](#_Toc143776914)

[3.1. Clearance Procedures 3](#_Toc143776915)

[3.1.1. Commitment for Employment – §117.10 (f)(1)(i)(ii)(f)(2)(3) 3](#_Toc143776916)

[3.2. Investigative Tiers and Processes 3](#_Toc143776917)

[3.3. Continuous Vetting 4](#_Toc143776918)

[3.4. Consultants – §117.10 (m) 4](#_Toc143776919)

[3.5. Pre-Employment Personnel Security Clearance Determination Actions 5](#_Toc143776920)

[3.6. SF 312 and other Nondisclosure Agreements 5](#_Toc143776921)

[3.7. Personnel Security Clearance Reciprocity 5](#_Toc143776922)

[4. Security Education – §117.12 5](#_Toc143776923)

[4.1. Initial Security Briefings – §117.12 (e)(f)(g) 5](#_Toc143776924)

[4.2. Insider Threat Training – §117.12 (g) 6](#_Toc143776925)

[4.3. Annual Security Briefings – §117.12 (k) 6](#_Toc143776926)

[4.4. Debriefings – §117.12 (l) 6](#_Toc143776927)

[4.5. Derivative Classification Training – §117.12 (h) (1) & (2) 6](#_Toc143776928)

[4.6. Special Security Briefings 7](#_Toc143776929)

[5. Security Reviews/Self-Inspections – §117.7 7](#_Toc143776930)

[5.1. Defense Counterintelligence and Security Agency 7](#_Toc143776931)

[5.2. Security Reviews 7](#_Toc143776932)

[5.3. Self-Inspections – §117.7 (h)(2) 7](#_Toc143776933)

[6. Individual Reporting Responsibilities - Security Executive Agent Directive 3 – §117.8 8](#_Toc143776934)

[6.1. How we establish the necessary processes and procedures to inform our cleared contractor personnel on reporting requirements related to SEAD 3 and the requirements for adverse information reporting as directed by the NISPOM Rule at section §117.8(c)(1) 8](#_Toc143776935)

[6.1.1. Foreign Travel 8](#_Toc143776936)

[6.1.2. Foreign Contacts 9](#_Toc143776937)

[6.1.3. Reportable Actions by Others 9](#_Toc143776938)

[6.1.4. Reportable Activities for Individuals with Access to Secret and Confidential Information, “L” Access or Holding a Non-Critical Sensitive Position 10](#_Toc143776939)

[6.1.5. Reportable Activities for Individuals with Access to Top Secret Information, “Q” Access or Holding a Critical or Special Sensitive Position 10](#_Toc143776940)

[6.2. How we receive, process, and manage the required reports and how these processes and procedures are implemented within our facility 12](#_Toc143776941)

[6.3. How a covered individual will alert the FSO or assigned designed of the reportable actions concerning other covered individuals 12](#_Toc143776942)

[7. Individual and Corporate Reporting Requirements – §117.8 13](#_Toc143776943)

[7.1. General 13](#_Toc143776944)

[7.2. Espionage/Sabotage 13](#_Toc143776945)

[7.3. Adverse Information – §117.118 (c)(1)(i)(ii) 14](#_Toc143776946)

[7.4. Suspicious Contacts – §117.18 (c)(2) 15](#_Toc143776947)

[7.5. Cleared Personnel Changes 15](#_Toc143776948)

[7.6. FCL Changes – §117.8 (c)(7) 16](#_Toc143776949)

[7.7. Security Equipment Vulnerabilities, Changes in Storage Capability, Inability to Safeguard Classified Material, and Dispositioned Material Previously Terminated 16](#_Toc143776950)

[7.8. Unsatisfactory Conditions of a Prime or Subcontractors 16](#_Toc143776951)

[7.9. Foreign Classified Contracts 16](#_Toc143776952)

[7.10. Loss, Compromise, or Suspected Compromise of Classified Information – §117.18(d) 17](#_Toc143776953)

[7.11. Individual Culpability Reports 17](#_Toc143776954)

[7.12. Cyber Incident Reports 18](#_Toc143776955)

[7.13. Reports to the Information Security Oversight Office 18](#_Toc143776956)

[8. Graduated Scale of Disciplinary Actions – §117.8 (e)(2) 19](#_Toc143776957)

[9. Defense Hotline – § 117.7 (j) 19](#_Toc143776958)

[10. Controlled Unclassified Information 20](#_Toc143776959)

[10.1. CUI Training and Awareness 20](#_Toc143776960)

[10.1.1. Initial Training 20](#_Toc143776961)

[10.1.2. Annual Refresher Training 20](#_Toc143776962)

[10.1.3. Training Records 21](#_Toc143776963)

[10.2. CUI Self-Inspection 21](#_Toc143776964)

[10.3. CUI Lifecycle 21](#_Toc143776965)

[10.4. Unauthorized Disclosure and CUI Misuse 21](#_Toc143776966)

[10.4.1. Unauthorized Disclosure 21](#_Toc143776967)

[10.4.2. CUI Misuse 21](#_Toc143776968)

[10.5. CUI Handling Responsibilities for Information Owners and End Users 22](#_Toc143776969)

[10.5.1. Compliance and Acknowledgment 22](#_Toc143776970)

[11. Marking Classified Information 22](#_Toc143776971)

[11.1. Classification Levels 22](#_Toc143776972)

[12. Classification and Marking Requirements – §117.13 23](#_Toc143776973)

[12.1. Original Classification 23](#_Toc143776974)

[12.2. Derivative Classification 23](#_Toc143776975)

[13. Classified Information Safeguarding 23](#_Toc143776976)

[13.1. Oral Discussions 23](#_Toc143776977)

[13.2. End-of-Day Checks 23](#_Toc143776978)

[13.3. Perimeter Controls 23](#_Toc143776979)

[13.4. Receiving Classified Material 23](#_Toc143776980)

[13.5. Storage of Classified Material 23](#_Toc143776981)

[13.6. Transmission of Classified Material 23](#_Toc143776982)

[13.7. Reproduction of Classified Material 23](#_Toc143776983)

[13.8. Destruction of Classified Material 24](#_Toc143776984)

[13.9. Retention of Classified Material 24](#_Toc143776985)

[14. Disclosure/Public Release – §117.15 24](#_Toc143776986)

[14.1. Disclosure 24](#_Toc143776987)

[14.2. Disclosure to Subcontractors and Other Contractors 24](#_Toc143776988)

[14.3. Disclosure to Ultimate Parent, Affiliates, and Subsidiaries 24](#_Toc143776989)

[14.4. Disclosure to Federal Agencies 25](#_Toc143776990)

[14.5. Disclosure to Foreign Persons 25](#_Toc143776991)

[14.6. Disclosure in Connection with Litigation 25](#_Toc143776992)

[14.7. Public Release 25](#_Toc143776993)

[14.8. Improperly Released Classified Information 26](#_Toc143776994)

[15. Visit and Classified Meetings 26](#_Toc143776995)

[15.1. Incoming Visits 26](#_Toc143776996)

[15.1.1. Classified Visits 26](#_Toc143776997)

[15.1.2. Classified Visits by U.S. Government Representatives 27](#_Toc143776998)

[15.1.3. Long Term Visitors 27](#_Toc143776999)

[15.1.4. Classified Meetings 27](#_Toc143777000)

[15.1.5. Escorting and IT Guest Access 27](#_Toc143777001)

[15.2. Outgoing Visits 28](#_Toc143777002)

[16. Subcontracting 28](#_Toc143777003)

[17. Information System Security 28](#_Toc143777004)

[18. International Security Requirements 28](#_Toc143777005)

[18.1. NATO Information Security Requirements 29](#_Toc143777006)

[18.1.1. NATO Briefings 29](#_Toc143777007)

[18.1.2. Subcontracting for NATO Contracts 29](#_Toc143777008)

[18.1.3. Further Distribution 29](#_Toc143777009)

[18.1.4. Visits 30](#_Toc143777010)

[19. Special Security Requirements 30](#_Toc143777011)

[19.1. Critical Nuclear Weapon Design Information 30](#_Toc143777012)

[19.1.1. Briefings 30](#_Toc143777013)

[19.1.2. Subcontractors 30](#_Toc143777014)

[19.1.3. Records 30](#_Toc143777015)

[19.2. COMSEC 31](#_Toc143777016)

[19.2.1. Clearance and Access Requirements. 31](#_Toc143777017)

[19.2.2. COMSEC Briefing and Debriefing 31](#_Toc143777018)

[19.2.3. U.S. Classified Cryptographic Information Access Briefing and Debriefing Requirements 32](#_Toc143777019)

[19.2.4. Subcontracting COMSEC work 32](#_Toc143777020)

[19.3. DHS CCIPP 32](#_Toc143777021)

[19.4. Other 32](#_Toc143777022)

[19.4.1. Intelligence Information 33](#_Toc143777023)

[19.4.2. Restricted Data, Formally Restricted Data, and Trans-classified Foreign Nuclear Information 33](#_Toc143777024)

[19.4.3. Naval Nuclear Propulsion Program 34](#_Toc143777025)

[20. Emergency Procedures 34](#_Toc143777026)

[20.1. Emergency Plan 34](#_Toc143777027)

[20.2. Emergency Contact Numbers 34](#_Toc143777028)

[21. Definitions 35](#_Toc143777029)

[22. Abbreviations and Acronyms 36](#_Toc143777030)

[23. Document Revision History 37](#_Toc143777031)

[24. Appendix A – SEAD 3 Reporting Matrix and Forms 38](#_Toc143777032)

# Introduction

This Standard Practice Procedures (SPP) describes E-volve Technology Systems, Inc.’s 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 (NISPOM) (32 Code of Federal Regulations (CFR) Part 117 NISPOM Rule), which takes precedence in instances of apparent conflict.

It is important for each employee to read this SPP to have a clear understanding of E-volve Technology Systems’ security policies and procedures and your role in protecting classified information.

# Facility Information

## Facility Clearance

A facility clearance (FCL) is an administrative determination that a facility is eligible for access to classified information or award of a classified contract. E-volve Technology Systems has a Top Secret facility clearance. The FCL is valid for access to classified information at the Top Secret or lower classification level.

## Facility Security Officer

Having a facility clearance E-volve Technology Systems 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 Rule and related Federal requirements for classified information.

Tanya D. Johnson is the FSO for E-volve Technology Systems and can be reached by email at tjohnson@e-volvetechsystems.com or by phone at 240-724-0104.

## 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 position in the entity with ultimate authority over the facility’s operations and the authority to direct actions necessary for the 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 U.S. Government (USG) locations. The SMO should be cleared to 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 requirements of 32 CFR Part 117 NISPOM
* Appoint a contractor employee or employees, in writing, as the FSO and the ITPSO
* Remain fully informed of the facility’s classified operations
* Make decisions based on classified threat reporting and thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information
* Retain accountability for the management and operations of the facility without delegating the accountability to a subordinate manager.

Deidre J. Boone is the SMO for our company and can be reached by email at dboone@e-volvetechsystems.com.

## Insider Threat Program Senior Official

Our company SMO has appointed the Insider Threat Program Senior Official (ITPSO) who should be cleared to the same level as the facility clearance. The ITPSO will complete training pursuant to 32 CFR Part §117.12.

Our company has established and will maintain and insider threat program, in accordance with 32 CFR Part §117.12(c) to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, 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 Program Plan.

Tanya D. Johnson is the ITPSO for our company and can be reached by email at tjohnson@e-volvetechsystems.com or by phone at 240-724-0104.

## 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. E-volve Technology Systems has *NOT* been approved to store classified material.

## 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 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 or personnel files, security records, supervisory files, 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 E-volve Technology Systems or its representatives or located in its offices.
* Providing access to employment and security records that are located at an offsite location, as applicable.
* Rendering other necessary assistance.
* DCSA Special Agents and Contract Investigators carry credentials identifying them as representatives of DCSA. They will present their credentials upon introduction. Further questions related to an Agent’s/Investigator’s identity or status should be directed to DCSA Security:

**Investigator Verification Hotline at 724-794-7186** (M-F / 7a-4p EST) or [**dcsa.boyers.bi.mbx.investigator-verifications@mail.mil**](mailto:dcsa.boyers.bi.mbx.investigator-verifications@mail.mil)

All employees should verify the identity of any Federal Agent/Investigator by asking to see their credentials before providing access to any information.

# Personnel Security Clearances **– §**117.10

## Clearance Procedures

E-volve Technology Systems 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 operational efficiency.

E-volve Technology Systems will utilize the DoD System of Record 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, Standard Form (SF) 86, through OPM’s current Electronic Questionnaire for Investigations Processing (e-QIP) system and then via the Defense Counterintelligence & Security Agency’s (DCSA) National Background Investigation Services (NBIS) Electronic Application (eAPP) component starting 1 October 2023.

In accordance with the NISPOM Rule, the FSO will notify the applicant in writing that the review of the   
SF 86 by the FSO or other contractor employee is for adequacy and completeness and information will be used for no other purpose within the entity. The use and disclosure by the U.S. Government, and by U.S. Government contractors operating systems of records on behalf of a U.S. Government agency to accomplish an agency function, of the information provided by the employee on the SF 86 is governed by the Privacy Act of 1974, as amended, and by the routine uses published by the USG in the applicable System of Records Notice. Information from the employee’s SF 86 shall not be shared within the entity and will not use the information for any purpose other than determining the adequacy and completeness of the SF 86.

### Commitment for Employment – §117.10 (f)(1)(i)(ii)(f)(2)(3)

While E-volve Technology Systems initiates the clearance process for employees, the government will make the determination of whether an individual is eligible to access classified information and grant the personnel clearance.

## Investigative Tiers and Processes

There are three investigative tiers:

1. One for positions designated as low risk, non-sensitive and allows physical and/or logical access to government facilities and computer systems.
2. One for positions designated as moderate risk, non-critical sensitive and allow access to classified at the L, Confidential (C), and Secret (S) levels.
3. One for positions designated as high risk, critical sensitive, special sensitive, and allow access to information classified at the Q, Top Secret (TS), and Sensitive Compartmented Information (SCI) levels.

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

* Automated sources such as automated record checks and inquiries.
* Interviews, if required, will cover areas of adjudicative concern.
* Information validated in a prior investigation, the results of which are not expected to change (e.g., 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 for specific Government Contracting Activity (GCA).

## Continuous Vetting

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 has replaced the requirement for Periodic Reinvestigations (PR).

Regardless of the level of access required, individuals holding security clearances are subject to a 5-year periodicity reporting requirement to maintain enrollment in the Continuous Vetting Program. Our FSO is responsible for reviewing all access records to ensure employees submit an updated SF-86, as required.

To determine when your next SF-86 is required to be submitted, the 5-years will be calculated by reviewing either the most recent investigation date ***or*** the most recent Continuous Evaluation (CE) enrollment date, reflecting as either “Enrolled or Continued Enrollment”.

* If an individual has a closed investigation date of 28 April 2019 and a CE ‘Enrollment’ date of 5 May 2020, the next reporting period (SF-86) will be May of 2025. The CE date is the most recent.
* If an individual has a closed investigation date of 16 June 2018 and a CE ‘Enrollment’ date of 3 Feb 2017, the next reporting period (SF-86) will be June 2023. The investigation date is most recent.
* If an individual has a closed investigation date of 8 Nov 2014 and a CE ‘Continued Enrollment’ date of 4 Jan 2021, the next reporting period (SF-86) will be Jan 2026. The CE date is the most recent.

## Consultants – §117.10 (m)

For security administration purposes, consultants are treated as employees of E-volve Technology Systems and must comply with this SPP and the 32 CFR Part 117 NISPOM Rule. Consultants will, however, be required to execute a Consultant Agreement which outlines any security responsibilities specific to the consultant.

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

## Pre-Employment Personnel Security Clearance Determination Actions

Per 32 CFR §117.10(f), if a potential employee requires access to classified information immediately upon start of employment, E-volve Technology Systems may submit the investigation request prior to the date of employment, provided:

* A written commitment for employment has been made by E-volve Technology Systems.
* The candidate has accepted the offer in writing.

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 for which they were hired.

## SF 312 and other Nondisclosure Agreements

Per 32 CFR §117.10(g), the SF 312 is a “Classified Information Nondisclosure Agreement (NDA)” between the USG and an individual who is determined eligible for access to classified information. Other Cognizant Security Agency (CSA) have additional sensitive compartmented information NDAs (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. The 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 312s into Defense Information System for Security (DISS) for retention prior to granting the employee access to classified information. If an employee refuses to sign the NDA(s), E-volve Technology Systems will deny the employee access to classified information and submit a report to the CSA in accordance with 32 CFR §117.18(c)(6).

## Personnel Security Clearance Reciprocity

Per 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 Security Executive Agent Directive (SEAD) 7.

# Security Education **– §**117.12

## Initial Security Briefings – §117.12 (e)(f)(g)

All cleared employees must receive an initial security briefing and sign an SF 312 NdA 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, including Insider Threat Awareness.
* Counterintelligence (CI) Awareness.
* Overview of Security Classification System.
* Employee reporting obligations and requirements, including insider threat.
* Cybersecurity training for all authorized information systems users in accordance with CSA-provided guidance.
* 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 a nondisclosure agreement.
* Insider Threat Training.
* Controlled Unclassified Information (CUI) training. *(While outside the requirements of the NISPOM Rule, when a classified contract includes provisions for CUI training, contractors will comply with those contract requirements)*.
* Overview of the SPP.

## Insider Threat Training – §117.12 (g)

The E-volve Technology Systems Insider Threat Program Senior Official Tanya D. Johnson ensures assigned insider threat program personnel and all cleared employees complete training consistent with applicable CSA provided guidance. See E-volve Technology Systems Insider Threat Program’s Insider Threat Training section for specific personnel functional or role requirements.

E-volve Technology Systems employees must complete insider threat awareness training annually. All newly cleared employees must complete insider threat awareness training before being granted access to classified information.

Insider threat awareness training covers current and potential threats in the work and personal environments and will include at a minimum:

* The importance of detecting insider threats by cleared employees and reporting suspected activity to the insider threat program designee.
* Methodologies of adversaries to recruit trusted insiders and collect information, in particular, within information systems.
* Indicators of insider threat behavior and procedures to report such behavior.
* CI and security reporting requirements, as applicable.

## Annual Security Briefings – §117.12 (k)

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

## Debriefings – §117.12 (l)

When a cleared employee no longer requires a security clearance or terminates employment with E-volve Technology Systems, the employee will be debriefed by the FSO or designee. Although signing the debriefing portion of the SF 312 is no longer a requirement, our FSO will provide a debriefing to remind the employee of their lifelong commitment to protect classified information.

## Derivative Classification Training – §117.12 (h) (1) & (2)

E-volve Technology Systems 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.

## Special Security Briefings

Some contracts contain requirements, often in the Contract Security Classification Specification (DD Form 254), for other special security briefings such as those indicated in Section 19. If E-volve Technology Systems has any of these requirements, the program manager should let the employees know to request a briefing from the FSO. If an employee gets read on to special programs at the customer location, the employee needs to notify the FSO in a timely manner.

# Security Reviews/Self-Inspections **– §**117.7

## Defense Counterintelligence and Security Agency

The DCSA is the government cognizant security office (CSO) which provides oversight of contractors’ procedures and practices for safeguarding classified defense information. Industrial Security Representatives of DCSA may contact the FSO in connection with the conduct of a security reviews of the facility, an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance to you and E-volve Technology Systems on security related issues.

Our assigned DCSA Field Office is:

Defense Counterintelligence & Security Agency

National Access Elsewhere Security Operations Center (NAESOC)

Phone: 888-282-7682 (Option #7)

email: [DCSA.NAESOC.generalmailbox@mail.mil](mailto:DCSA.NAESOC.generalmailbox@mail.mil)

## Security Reviews

E-volve Technology Systems will be assessed by the DCSA on a periodic basis. During this time, DCSA Industrial Security Representative (ISR) will review our security processes and procedures to ensure compliance with the 32 CFR Part 117 NISPOM Rule, and interview E-volve Technology Systems employees to assess the effectiveness of the security program. Your cooperation with DCSA during the Security Review (SR) is required.

## Self-Inspections – §117.7 (h)(2)

E-volve Technology Systems security staff will also perform a self-inspection, similar to the DCSA Security Review. This self -inspection should be done at least once annually but no more than 365 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, E-volve Technology Systems employees will be interviewed. 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 the National Industrial Security System (NISS).

# Individual Reporting Responsibilities - Security Executive Agent Directive 3 **– §**117.8

## How we establish the necessary processes and procedures to inform our cleared contractor personnel on reporting requirements related to SEAD 3 and the requirements for adverse information reporting as directed by the NISPOM Rule at section §117.8(c)(1)

All covered employees are required to report any of the following information to the FSO. Our FSO, Tanya D. Johnson, can be reached by email at tjohnson@e-volvetechsystems.com or by phone at 240-724-0104. Covered individuals do not just have to report their own behavior; they are obligated to report similar information if they observe it in others.

For specific details, refer to: [SEAD-3-Reporting.pdf (dni.gov)](https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf) and [ISL2021-02\_SEAD-3.pdf (dcsa.mil)](https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL2021-02_SEAD-3.pdf)

The FSO includes the above reporting requirements in our initial and refresher briefings.

### Foreign Travel

Unofficial foreign travel is required to be reported. Unofficial foreign travel is defined as all travel other than that defined by “official foreign travel,” and includes any foreign travel conducted before, during, or after official foreign travel, and that does not meet the criteria of “official foreign travel” as stipulated below.

* Deviations from submitted travel itinerary must be reported by the cleared employee to the FSO or assigned designee within five business days of return.
* Unplanned day trips to Canada or Mexico by persons residing in the U.S. must be reported to the FSO or assigned designee within five business days of return.
* Unofficial foreign travel under emergency circumstances does not require pre-approval, however, the cleared employee should advise their FSO of the emergency foreign travel prior to departure. Reporting, consisting of a complete travel itinerary, shall be accomplished within five business days of return.
* Cleared employees who are employed by E-volve Technology Systems and who reside abroad are required to report all unofficial foreign travel outside of the foreign country in which they reside. If reports of aggregated unofficial foreign travel are submitted for such covered individuals, the reporting period for that covered individual must not exceed 120 days.
* Unofficial foreign travel that is not reported in advance and does not fall under the above circumstances, shall be reported to the FSO, or assigned designee as soon as possible after the travel occurs.

E-volve Technology Systems requires pre-approval prior to unofficial foreign travel in accordance with SEAD 3. DoD considers unofficial foreign travel by a covered individual under DoD NISP security cognizance as approved when the first set of items one through four occur as follows:

1. The cleared employee notifies the Facility Security Officer or assigned designee before foreign travel. If notification does not occur in advance, the covered individual must notify the FSO or designee as soon as possible after the travel occurs, not to exceed five business days.

2. The cleared employee submits a complete travel itinerary to FSO or designee using Appendix A Form 01 – Foreign Travel and the FSO or designee reports the travel prior to the unofficial foreign travel in DISS or subsequent system of record, such as NBIS when component becomes available.

3. The FSO or designee provides the cleared employee with the National Counterintelligence and Security

Center (NCSC) “Safe Travels” resource: [Counterintelligence\_Tips\_Safe\_Travels.pdf (dni.gov)](https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf) for required review.

4. If applicable, the FSO or designee coordinates with a DCSA Counterintelligence Special Agent (CISA) for appropriate pre-foreign travel briefings when the covered individual is traveling to a foreign country listed in the Director of National Intelligence’s Worldwide Threat Assessment of the U.S. Intelligence Community which is available at [Reports & Publications (dni.gov)](https://www.dni.gov/index.php/newsroom/reports-publications).

Additionally, our FSO or designee will:

1. Provide employee notification and links to the current US State Department travel advisories for their reported destination(s). Advisories are listed at: [Travel Advisories (state.gov)](https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/).

2. Coordinate with DCSA CISA for post-foreign travel debriefings when cleared employee reports any contact with foreign intelligence entities or other foreign travel anomalies during the foreign travel event.

3. If submitting reports of aggregated unofficial foreign travel for covered individuals who routinely travel, this reporting period must not exceed 120 days. In this case, the travel is approved if the FSO refers the covered individual to the NCSC “Safe Travels” resource link: [Counterintelligence\_Tips\_Safe\_Travels.pdf (dni.gov)](https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf) at least annually for required review.

4.The FSO or designee will ensure that any foreign travel conducted by a cleared employee who is terminating their relationship with E-volve Technology Systems is reported immediately.

### Foreign Contacts

* Unofficial contact with a known or suspected foreign intelligence entity. The FSO will also report this activity directly to the DCSA CISA.
* Continuing association with known foreign nationals that involves bonds of affection, personal obligation, or intimate contact.
* Any contact with a foreign national involving the exchange of personal information.

### Reportable Actions by Others

To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered employees will alert the FSO or designee to the following reportable activities of other covered individuals that may be of potential security or counterintelligence concern:

* An unwillingness to comply with rules and regulations or to cooperate with security requirements.
* Unexplained affluence or excessive indebtedness.
* Alcohol abuse.
* Illegal use or misuse of drugs or drug activity.
* Apparent or suspected mental health issues, where there is reason to believe it may impact the covered individual’s ability to protect classified information or other information specifically prohibited by law from disclosure.
* Criminal conduct.
* Any activity that raises doubt as to whether another covered individual’s continued national security eligibility is clearly consistent with the interests of national security.
* Misuse of U.S. Government property or information systems.

### Reportable Activities for Individuals with Access to Secret and Confidential Information, “L” Access or Holding a Non-Critical Sensitive Position

In addition to the reporting requirements in 6.1.1, 6.1.2 and 6.1.3, individuals with access to Secret and Confidential Information, “L” Access or Holding a Non-Critical Sensitive Position shall report:

1. Foreign Activities.
2. Application for and receipt of foreign citizenship.
3. Application for, possession, or use of a foreign passport or identity card for travel.
4. Other Reportable Activities.
5. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.
6. Media contacts if the media seeks access to classified information or information otherwise prohibited from public disclosure, and if an associated investigation/inquiry reveals a mishandling and/or unauthorized disclosure of classified information.
7. Arrests.
8. Bankruptcy or over 120 days delinquent on any debt.
9. Alcohol and drug related treatment.
10. Cryptocurrency – Ownership of foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges.
11. Psychological and emotional health conditions that involve the following situations:

* A court or administrative agency issued order declaring the individual to be mentally incompetent.
* A court or administrative agency ordering the individual to consult with a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.).
* Hospitalization of the individual for a mental health condition.
* Diagnosis of the individual by a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.) of psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial personality disorder.
* Occasions within the last seven years where the individual did not consult with a medical professional before altering, discontinuing, or failing to start a prescribed course of treatment for any of the above diagnoses. Details of any current treatment for the above diagnoses must be reported.
* Any mental health or other health condition that the employee feels substantially and adversely affects their judgment, reliability, or trustworthiness regardless of current symptoms.

### Reportable Activities for Individuals with Access to Top Secret Information, “Q” Access or Holding a Critical or Special Sensitive Position

In addition to the reporting requirements in 6.1.1, 6.1.2 and 6.1.3, Individuals with Access to TS and C Information, “Q” Access or Holding a Critical or Special Sensitive Position shall report:

1. Foreign Activities.
2. Direct involvement in a foreign business.
3. Foreign bank accounts.
4. Ownership of foreign property.
5. Application for and receipt of foreign citizenship.
6. Application for, possession, or use of a foreign passport or identity card for travel.
7. Voting in a foreign election.
8. Adoption of non-U.S. citizen children.
9. Other Reportable Activities.
10. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.
11. Media contacts if the media seeks access to classified information or information otherwise prohibited from public disclosure, and if an associated investigation/inquiry reveals a mishandling and/or unauthorized disclosure of classified information.
12. Arrests.
13. Financial Anomalies: Including but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain.
14. Foreign National Roommate(s) – Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.
15. Cohabitant(s): A person with whom the covered individual resides, and shares bonds of affection, obligation, or other commitment as opposed to a person with whom the covered individual resides for reasons of convenience (e.g., a roommate).
16. Marriage: All civil marriages, legally recognized civil unions, and legally recognized domestic partnerships.
17. Alcohol and drug related treatment.
18. Cryptocurrency – Ownership of foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges.
19. Psychological and emotional health conditions that involve the following situations:

* A court or administrative agency issued order declaring the individual to be mentally incompetent.
* A court or administrative agency ordering the individual to consult with a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.).
* Hospitalization of the individual for a mental health condition.
* Diagnosis of the individual by a mental health professional (psychiatrist, psychologist, licensed clinical social worker, etc.) of psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial personality disorder.
* Occasions within the last seven years where the individual did not consult with a medical professional before altering, discontinuing, or failing to start a prescribed course of treatment for any of the above diagnoses. Details of any current treatment for the above diagnoses must be reported.
* Any mental health or other health condition that the employee feels substantially and adversely affects their judgment, reliability, or trustworthiness regardless of current symptoms.

## **How we receive, process, and manage the required reports and how these processes and procedures are implemented within our facility**

Covered personnel are instructed to make initial reports to the FSO, or assigned designee, via phone or preferably by email simply stating the individual has a report to make and the type of report. If an in-person meeting takes place, the FSO, or assigned designee, will request a follow up email for our records. The FSO, or assigned designee, will forward the appropriate SEAD 3 reporting form (see Appendix A – SEAD 3 Reporting Forms) to the employee for completion. These SEAD 3 Reporting Forms contain the same data elements required in SEAD 3. This allows our FSO to collect all the data required to submit the report to the GCA. The employee will complete the reporting form and return it via secure email, or password protected email, to the FSO or assigned designee. The FSO or assigned designee will review the information provided on the form, compare it to Industrial Security Letter 2021-02 and the SEAD 3 Industry Reporting Desktop Aid: [PowerPoint Presentation (dcsa.mil)](https://www.dcsa.mil/Portals/91/Documents/CTP/tools/SEAD3_REPORTING_DESKTOP_AID_FOR_CLEARED_INDUSTRY.pdf), enter the information into DISS as a Customer Service Report (CSR) or Incident Customer Service Report, and file the reporting form in the individual’s security file. If the report is stored electronically, the FSO will ensure all reports containing Personally Identifiable Information (PII) or CUI are stored in accordance with appropriate government guidelines. The FSO or assigned designee will monitor DISS for a response from DCSA and will inform the employee of the resulting action, as appropriate.

## **How a covered individual will alert the FSO or assigned designed of the reportable actions concerning other covered individuals**

To ensure the protection of classified information or other information specifically prohibited by law from disclosure, our FSO will alert each covered individual during initial and refresher briefings to the following activities of other covered individuals that may be of potential security or counterintelligence concern. (SEAD 3, F.3). Further, our FSO will advise each covered individual to make initial reports to the FSO, or assigned designee, via phone or preferably by email simply stating the individual has a report to make and the type of report. If an in-person meeting takes place, the FSO will request a follow-up email for our records. The FSO, or assigned designee, will forward the appropriate SEAD 3 reporting form (see Appendix A – SEAD 3 Reporting Forms -- Form 21 - Reportable Actions by Others) to the employee for completion. The employee will complete the reporting form and return it via secure email or password protected email to the FSO or assigned designee. The FSO or assigned designee will review the form, enter the information into DISS as a CSR or Incident Customer Service Report, and file the reporting form in the individual’s security file. If the report is stored electronically, the FSO will ensure all reports containing PII or CUI are stored in accordance with appropriate government guidelines. The FSO or assigned designee will monitor DISS for a response from DCSA and will coordinate any subsequent clearance actions with the subject of the report, as required.

a. An unwillingness to comply with rules and regulations or to cooperate with security requirements.

b. Unexplained affluence or excessive indebtedness.

d. Alcohol abuse

e. Illegal use or misuse of drugs or drug activity.

f. Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual’s ability to protect classified information or other information specifically prohibited by law from disclosure.

g. Criminal conduct.

h. Any activity that raises doubts as to whether another covered individual’s continued national security eligibility is clearly consistent with the interests of national security.

i. Misuse of U.S. Government property or information systems.

# Individual and Corporate Reporting Requirements **– §**117.8

## General

In accordance with SEAD 3 and CSA-provided guidance to supplement unique CSA mission requirements, E-volve Technology Systems and our cleared employees will:

1. Report certain events that may influence the status of the entity's or an employee's eligibility for access to classified information; report events that indicate an insider threat to classified information or to employees with access to classified information; report events that affect proper safeguarding of classified information; and report events that indicate classified information has been, or is suspected to be, lost, or compromised.
2. E-volve Technology Systems has established internal procedures to ensure employees with eligibility for access to classified information are aware of their responsibilities for reporting pertinent information to the FSO. These procedures are documented in this SPP and are included in our initial and annual refresher briefings. E-volve Technology Systems will:
3. Provide reports to the FBI, or other Federal authorities as required by the NISPOM Rule, the terms of a classified contract or other agreement, and by U.S. law.
4. Provide complete information to enable the CSA to ascertain whether classified information is adequately protected.
5. Submit reports to the FBI, the CSA, or the Information Security Oversight Office (ISOO) as specified in paragraphs (b), (c), and (g) of the NISPOM Rule.
6. Appropriately mark reports containing classified information in accordance with NISPOM Rule §117.14.
7. Clearly mark a report containing information submitted in confidence as containing that information. When reports contain information pertaining to an individual, 5 U.S.C. 552a (also known as and referred to in this rule as “The Privacy Act of 1974, as amended,”) permits the withholding of certain information from the individual in accordance with specific exemptions, which include authority to withhold release of information to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the USG under an express promise that the identity of the source would be held in confidence.

## Espionage/Sabotage

Employees should report to the FSO immediately any information concerning existing or threatened espionage, sabotage, or subversive activities. Examples of these 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 war materials, premises, or utilities.
* Destroying or damaging national materials, premises, or utilities.
* Producing defective national defense materials, 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.

The FSO will immediately contact the local FBI office with a courtesy copy to DCSA. The local FBI office can be reached at (202) 278-2000.

## Adverse Information – §117.118 (c)(1)(i)(ii)

E-volve Technology Systems is required to report adverse information coming to our attention concerning any of our employees determined to be eligible for access to classified information, in accordance with the NISPOM Rule, SEAD 3, and CSA-provided guidance. We will not make reports based on rumor or innuendo.

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 himself, herself, or another cleared individual to the FSO. 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 a mental institution.

Cryptocurrency- ownership of foreign state-backed, hosted, or managed cryptocurrency and ownership of cryptocurrency wallets hosted by foreign exchanges.

Use of illegal substances or excessive use of alcohol or other prescription drugs.

Bankruptcy, excessive debt, including garnishments on employee’s wages.

Unexplained affluence/wealth, any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain.

Unexplained absence from work for periods of time that is unwarranted or peculiar.

Criminal convictions involving a gross misdemeanor, felony, or court martial.

Termination for cause.

Must report being over 120 days delinquent on debt.

Any arrest, regardless of whether charges were filed.

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.

The FSO will report this information immediately to the DCSA Vetting Risk Operations (VRO) office via the incident report function in the current clearance database of record.

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

## Suspicious Contacts – §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 foreign national resume where the job advertisement states that a clearance is required.
* Receipt of 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 obligation 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 our DCSA ISR.

## Cleared Personnel Changes

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

* Death.
* Change in name.
* Change in marital status.
* Termination of employment.
* Change in citizenship.
* Access to classified information is no longer needed.
* No longer wish to be processed for a personnel clearance, continue an existing clearance, or perform classified work.
* Refusal by an employee to sign the SF 312, “Classified Information Nondisclosure Agreement”
* Citizenship by naturalization for non-US citizens granted a Limited Access Authorization.

The FSO will report this information immediately to the DCSA VRO office using the current clearance database of record.

## FCL Changes – §117.8 (c)(7)

Per 32 CFR §117.18 (c)(7), company leadership must report facility changes to the FSO which include:

* Change of ownership or control of the contractor, including stock transfers that affect control of the entity.
* Change of operating name or address of the entity or any of its locations determined eligible for access to classified information.
* Any change to the information previously submitted for Key Management Personnel (KMP).
* Any action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change 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).

## Security Equipment Vulnerabilities, Changes in Storage Capability, Inability to Safeguard Classified Material, and Dispositioned Material Previously Terminated

Personnel must immediately report to the FSO any 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 DSCA ISR via email.

## Unsatisfactory Conditions of a Prime or Subcontractors

Per 32 CFR §117.18 (c)(10) and (c)(14) with respect to responsibilities for reporting to be submitted to DSCA, each subcontractor will be considered as a prime contractor in relation to its own employees or subcontractor(s). Subcontractors will also notify their 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 subcontractors.

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

The employee will report to the FSO any of the above conditions. The FSO will report this information immediately to their DCSA ISR.

## Foreign Classified Contracts

Per 32 CFR §117.18 (c)(12) and (c)(13), we must report any pre-contract negotiations or award not placed through DCSA or USG contracting activity that involves or may involve the release or 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 information from foreign interests that is not received through Government channels.

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

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

## **Loss, Compromise, or Suspected Compromise of Classified Information** – §117.18(d)

Cleared personnel must immediately report to the FSO the loss, compromise, or suspected compromise of classified information. The FSO will report this information immediately to their DCSA ISR. The report will be made initially via email.

Each CSA may provide additional guidance concerning the reporting period. If the contractor is located on a USG facility, the contractor will submit the report to the CSA and to the head of the USG facility.

(1) Preliminary inquiry. Immediately upon receipt of a security violation report involving classified information, E-volve Technology Systems will initiate a preliminary inquiry to ascertain all the circumstances surrounding the presumed loss, compromise, or suspected compromise, including validation of the classification of the information.

(2) Initial report. If E-volve Technology Systems’ preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, E-volve Technology Systems will promptly submit an initial report of the incident unless otherwise notified by the CSA.

(3) Final report. When the investigation has been completed, E-volve Technology Systems will submit a final report to the CSA which, in turn, will follow CSA procedures to notify the applicable GCA. The report will include:

(i) Material and relevant information that was not included in the initial report.

(ii) The full name and social security number of the individual or individuals primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible.

(iii) A statement of the corrective action taken to preclude a recurrence.

(iv) Disciplinary action taken against the responsible individual or individuals, if any.

(v) Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur.

(4) Employee information in compromise cases. When requested by the CSA, E-volve Technology Systems will report information concerning an employee or other individual, determined to be responsible for the incident, when the information is needed by the CSA for the loss, compromise, or suspected compromise of classified information.

## **Individual Culpability Reports**

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 for E-volve Technology Systems’ 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 questionable judgment, irresponsibility, negligence, or carelessness.

The FSO will report this information immediately to the DCSA VRO office via the incident report function in the clearance database of record.

## **Cyber Incident Reports**

Per 32 CFR §117.8 (f), as a cleared defense contractor and pursuant to 10 U.S.C. 391 and 393 and Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, E-volve Technology Systems must report cyber incidents, which can include certain activities occurring on unclassified information systems. DoD will provide detailed reporting instructions for contractors affected by these references via industrial security letter in accordance with DoDI 5220.22.

E-volve Technology Systems will immediately report any cyber incident on a classified covered information system that has been approved by DCSA to process classified information, including at a minimum:

* A description of the technique or method used in the cyber incident.
* A sample of the malicious software involved in the cyber incident, if discovered and isolated by the Cleared Defense Contractor (CDC).
* A summary of information in connection with any DoD program that has been potentially compromised due to the cyber incident.

E-volve Technology Systems will safeguard, use, and disseminate reported information in a manner consistent with DoD procedures governing the handling of such information pursuant to Public Law 112-239 and 10 U.S.C. 391.

E-volve Technology Systems will report cyber incidents involving classified foreign government information to the Director, Defense Technology Security Administration at DoD.

E-volve Technology Systems must allow, upon request by DoD personnel, access by DoD personnel to E-volve Technology Systems equipment or information that is necessary to conduct forensic analysis of reportable cyber incidents in addition to any E-volve Technology Systems analysis conducted. This is to determine whether DoD program information was successfully exfiltrated from a E-volve Technology Systems’ network or information system, and what it was.

The employee will report to the FSO any of the above conditions. The FSO will notify the ISSM or IT Manager, whichever is applicable.

The ISSM or IT Manager, or FSO will report this information immediately into the DIBNET located at [Defense Industrial Base (DIB) Cybersecurity Portal](https://dibnet.dod.mil/portal/intranet/).

## **Reports to the Information Security Oversight Office**

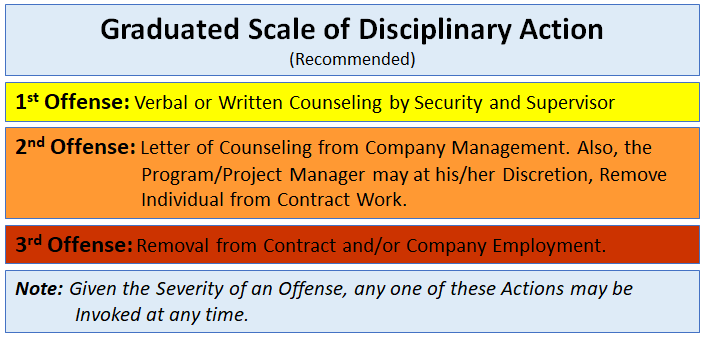
Per 32 CFR §117.8 (g), E-volve Technology Systems must report to the Director of ISOO (National Security Archives and Records Administration) instances of redundant or duplicative security review and audit activity by DCSA for resolution. If there is an existing determination of an entity’s eligibility for access to classified information and another CSA is requiring duplicating processing to determine an entity’s eligibility for access to classified information, E-volve Technology Systems will 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. The FSO may initiate this process by calling 1-86-NARA-NARA or 1-866-272-6272.

# Graduated Scale of Disciplinary Actions **– §**117.8 (e)(2)

E-volve Technology Systems will use the following graduated scale of disciplinary actions as a guide in determining appropriate administrative actions to assign to security violations:



The FSO has the right to skip the graduated scale of discipline. Some situations may warrant bypassing some or all the steps outlined in the graduated scale of discipline. When it has been determined that an employee has committed a security violation, that employee will be rebriefed by the FSO to address the specific violation.

Disciplinary action by senior management will be based on the severity and frequency of any offense; however senior management reserves the right to dismiss an employee for any offense. Based on the severity of the violation, the FSO will be required to notify the DCSA by submitting an “Incident Report” even if the employee is ultimately terminated.

# **Defense Hotline – § 117.7 (j)**

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.

The Defense Hotline has received over a quarter million calls and letters. Many cases resulted in safer products and equipment for our military personnel and Defense Department employees.

Any E-volve Technology Systems employee who witnesses what he or she believes to be a violation of ethical standards and/or the law, including but not limited to fraud, waste, or abuse of authority, potential leaks of classified information, or potential acts of terrorism, should report such conduct through his or her chain of command, respective service Inspector General, or directly to the Inspector General of the **Department of Defense** **Hotline** at **800-424-9098**. The violations that follow should be reported to the Defense Hotline:

* Threats to homeland security.
* Unauthorized disclosures (Leaks).
* Human trafficking.
* Contract and procurement irregularities.
* Cost/labor mischarging.
* Defective pricing.
* Defective parts.
* Bid rigging.
* Product substitution.
* Spare parts overpricing.
* Bribery and acceptance of gratuities.
* Significant cases of mismanagement.
* Conflicts of interest.
* Travel (TDY/TAD) fraud.
* Abuse of authority.
* Theft and abuse of Government property.
* Military reprisal (violations of the Whistleblower Protection Act involving service members).
* Violations of the Whistleblower Protection Act involving defense contractor employees and non-appropriated fund employees.
* Improper referrals of military personnel for mental health evaluations.
* Gross waste of funds.

**DEFENSE HOTLINE**

**THE PENTAGON**

**WASHINGTON, DC 20301-1900**

**TELEPHONE: 800-424-9098**

[**http://www.dodig.mil/hotline**](http://www.dodig.mil/hotline)

# Controlled Unclassified Information

## 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 DCSA Center for Security Excellence (CDSE) provides CUI training that is available to Industry (IF141.06). This course fulfills CUI training requirements for industry when it is required by Government Contracting Agencies for contracts with CUI requirements (and for all employees that handle CUI as part of their duties).

### Annual Refresher Training

E-volve Technology Systems 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.

### Training Records

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

## CUI Self-Inspection

The CUI Manager will review the CUI Self-Inspection Appendix to assist in the initial establishment of E-volve Technology Systems’ CUI program. Once established, the CUI Self-Inspection Appendix should be considered to self-assess the CUI security procedures, determine compliance, and effectiveness of E-volve Technology Systems’ CUI program, and identify any deficiencies/weaknesses. The self-inspection results must be documented.

## CUI Lifecycle

CUI follows a lifecycle similar to all protected information. While the designation of certain types of information requiring safeguarding and dissemination may be new, the process should be familiar.



## Unauthorized Disclosure and CUI Misuse

### Unauthorized Disclosure

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

### CUI Misuse

Misuse of CUI is an occurrence that takes place when someone uses CUI in a manner not in accordance with the policy contained in E.O. 13556, 32 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 international 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 Manager is responsible for conducting a preliminary Administrative Inquiry (AI). The purpose of the preliminary inquiry is to secure the CUI information, quickly gather the available facts, and determine if CUI information was subject to compromise. If the CUI Manager concludes, based on the preliminary AI, that no loss, compromise, or suspected compromise occurred, the CUI Manager has the responsibility to finalize the inquiry.

## CUI Handling Responsibilities for Information Owners and End Users

All E-volve Technology Systems 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 computers (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).

### Compliance and Acknowledgment

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

Employees of E-volve Technology Systems should contact the CUI Manager if there are any questions about any of the sections of this document.

# Marking Classified Information

## 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.

# Classification and Marking Requirements **– §**117.13

## 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 DD Form 254 and Security Classification Guidance applicable to each classified contract.

## Derivative Classification

E-volve Technology Systems 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.

# Classified Information Safeguarding

## Oral Discussions

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## End-of-Day Checks

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Perimeter Controls

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Receiving Classified Material

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Storage of Classified Material

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Transmission of Classified Material

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Reproduction of Classified Material

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Destruction of Classified Material

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

## Retention of Classified Material

E-volve Technology Systems is *NOT* currently approved for classified safeguarding. This section will be completed if/when we are approved for safeguarding.

# Disclosure/Public Release **– §**117.15

## Disclosure

E-volve Technology Systems 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. E-volve Technology Systems personnel shall continue the classification until formally advised to the contrary.

## Disclosure to Subcontractors and Other Contractors

Per 32 CFR §117.15(h)(2), E-volve Technology Systems 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.

E-volve Technology Systems will convey appropriate classification guidance for the classified information to be disclosed with the subcontract in accordance with 32 CFR §117.13.

E-volve Technology Systems may only disclose classified information to the subcontractor if DCSA (or other applicable CSA has already:

* Pre-determined 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.

32 CFR §117.15(h)(6), E-volve Technology Systems may *NOT* disclose any classified information to any other contractor except in furtherance of a contract, subcontract, or other GCA purpose without authorization of the GCA, if such authorization is required by contract.

## Disclosure to Ultimate Parent, Affiliates, and Subsidiaries

E-volve Technology Systems may *NOT* disclose any classified information to its Parent, any Ultimate Parent Affiliates, or subsidiaries unless DCSA (or other applicable CSA) makes an entity eligibility determination including an approval for storage if required. This has NOT occurred so E-volve Technology Systems may NOT disclose any classified information to its Parent, any Ultimate Parent Affiliates, or subsidiaries.

## Disclosure to Federal Agencies

Per 32 CFR §117.15(h)(2), E-volve Technology Systems may *NOT* disclose classified information received or generated under a contract from one agency to another federal agency unless specifically authorized by the agency that has classification jurisdiction over the information.

## Disclosure to Foreign Persons

Per 32 CFR §117.15(h)(2), E-volve Technology Systems may *NOT* disclose classified information to foreign persons unless specified by the contract and release of information is authorized in writing by the government agency having classification jurisdiction over the information involved, i.e., the Department of Energy (DOE) for Formally Restricted Data (FRD) (also see 32 CFR §117.23), the NSA for Communication Security (COMSEC), the Director of National Intelligence (DNI) for SCI, and all other executive branch departments and agencies for classified information under their respective jurisdictions.

## Disclosure in Connection with Litigation

Per 32 CFR §117.15(h)(7), E-volve Technology Systems may *NOT* disclose classified information to:

* Attorneys hired solely to represent E-volve Technology Systems in any civil or criminal case in federal or State courts unless the disclosure 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.

## Public Release

Per 32 CFR §117.15(h)(8), E-volve Technology Systems may *NOT* disclose classified information to the public. Contact the FSO to determine the process for obtaining prior GCA approval.

E-volve Technology Systems may *NOT* disclose unclassified information pertaining to a classified contract to the public without prior review and clearance as specified 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. Further, 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, E-volve Technology Systems 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 the 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 hiring 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.

E-volve Technology Systems may *NOT* disclose information that has been declassified, if the information is comingled with CUI, or qualifies as CUI once declassified. In such instances, the E-volve Technology Systems will mark and protect it as CUI until it is reviewed for public release or decontrolled pursuant to 32 CFR 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.

## Improperly Released Classified Information

Per 32 CFR §117.13(g), 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, E-volve Technology Systems 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 proprietary of continued classification in these cases to the immediate attention of the GCA.
* Notify DCSA, or the applicable GCA, if an employee downloads the improperly released classified information to determine how to resolve a data spill.

# Visit and Classified Meetings

## Incoming Visits

All incoming classified visits must be approved in advance of the visit by the FSO. The FSO will verify each visitor’s security status prior to allowing classified access. 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 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.

### Classified 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 to a USG facility.

E-volve Technology Systems does *NOT* currently have approval to store 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 our locations.

E-volve Technology Systems 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 need to know determination prior to the disclosure of any classified information at a level that is consistent with visit purpose for both incoming and outgoing visits.

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. Need to know is generally based on a contractual relationship between the contractors. In other circumstances, disclosure of the information will be based on an assessment that the receiving contractor has a bona fide need to access the information in furtherance of a GCA purpose.

For visits to USG or other contractor facilities, E-volve Technology Systems employees must allow ample time for visit authorization letter request 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.

### Classified Visits by U.S. Government Representatives

Representatives of the USG, when acting in their official capacities as inspectors, investigators, or auditors, may visit E-volve Technology Systems facility, provided these representatives present appropriate USG credentials upon arrival.

### Long Term Visitors

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

E-volve Technology Systems employees at USG locations will follow the security requirements of the host facility. This does not relieve E-volve Technology Systems from security oversight of our employees who are long-term visitors at USG locations.

### Classified Meetings

Per 32 CFR §117.16(b), “Classified Meetings” concern 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 conferences increases security risks. Classified disclosure at such meetings may occur when it serves a government purpose and adequate security measures have been provided in advance.

E-volve Technology Systems 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 E-volve Technology Systems plans to conduct classified meetings as a cleared contractor host, a USG agency must authorize the meeting and will assume security jurisdiction. Such meetings will comply with the requirements in 32 CRF §117.16(b).

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

### Escorting and IT Guest Access

E-volve Technology Systems has no plans to entertain visitors at its facility. However, should the need arise the E-volve Technology Systems employee visitor host or their designee will escort the visitor to meetings in the E-volve Technology Systems facility. 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 the room/conference room during a break if the escort/host has a visual line of sight with the visitor. E-volve Technology Systems will not provide a key, keycard, or fob for facility access to visitors.

We don’t anticipate the need, but should there ever be a need, E-volve Technology Systems will only grant visitors access to the guest IT network, which is separate from the E-volve Technology Systems network. The guest IT network does not permit access to E-volve Technology Systems information.

## Outgoing Visits

All classified visits require advance notification to, and approval of, the place being visited. When it becomes necessary for employees of E-volve Technology Systems 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, the access level required, and the person to be contacted. Ample time must be allowed to permit the visit authorization request to be prepared, submitted via DISS to the contractor/agency, and processed by their visitor control.

# Subcontracting

If E-volve Technology Systems decides to subcontract any work under a classified contract, it will comply with the security requirements of 32 CFR §117.17. The subcontractor must possess an appropriate entity eligibility determination and a classified information safeguarding capability if possession of classified information will be required. E-volve Technology Systems 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.

# Information System Security

E-volve Technology Systems is not approved to process information on any computer or other electron device. If we have formal approval/accreditation in the future from a GCA, this section will be updated, an ISSM will be appointed, and a separate System Security Plan will be maintained for all classified information systems.

If you have any questions as to whether a system is approved, please contact the FSO or ISSM.

# International Security Requirements

E-volve Technology Systems currently has or may have approval to disclose classified U.S. information to foreign interests in the future. If current or future contracts require this kind of disclosure, E-volve Technology Systems will implement procedures and comply with 32 CFR §117.19 as described in the following subsections.

The transfer of articles, services, and related data to a foreign person, within or outside the United States, or the movement of such material or information to any destination outside of the legal jurisdiction of the United States constitutes an export. Depending on the nature of the articles or data, most exports are pursuant to 22 U.S.C. chapter 39, also known and referred to in this part as “Armed Export Control Act,” 50 U.S.C. 4801 et seq., also known as the “Export Control Reform Act of 2018” and the AEA. This section applies to those exports that involve classified information. 32 CFR §117.19 provides security requirements related to:

* Bilateral security agreements.
* Industrial security agreements negotiated with foreign governments.
* International agreements.
* Classified symposia, seminars, exhibitions, and conferences.
* Classified visits by foreign nationals to the contractor location.
* Temporary export for demonstration purposes.
* Direct commercial arrangements for subcontracting.
* Foreign government information.
* Contactor operations abroad.
* North Atlantic Treaty Organization (NATO) information.
* Treaties with Australia and the United Kingdom involving classified information.

## NATO Information Security Requirements

If E-volve Technology Systems has NATO information security requirements, we will comply with the following procedures from 32 CFR §117.19.

### NATO Briefings

Before having access to NATO classified information, E-volve Technology Systems will give employees a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO classified information. A representative of the CSA will give the initial briefing to E-volve Technology Systems. E-volve Technology Systems will conduct annual refresher briefings.

* When access to NATO classified information is no longer required, E-volve Technology Systems will debrief the employees. The employees will sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information.
* E-volve Technology Systems will maintain certificates, current year plus two previous years for NATO Secret and Confidential, and current year plus previous three years for COSMIC TS and all ATOMAL information. E-volve Technology Systems will maintain a record of all NATO briefings and debriefings in the CSA-designated database.

### Subcontracting for NATO Contracts

E-volve Technology Systems will obtain prior written approval from the NATO contracting activity and a NATO Facility Security Clearance Certificate (FSCC) must be issued prior to awarding the subcontract. E-volve Technology Systems will forward the request for approval through the CSA.

### Further Distribution

E-volve Technology Systems will not release or disclose NATO classified information to a third party or outside the E-volve Technology Systems’ facility for any purpose without the prior written approval of the contracting agency.

### Visits

NATO visits will be handled in accordance with the requirements in §117.19(e). A NATO Certificate of Security Clearance will be included with the visit request.

* NATO Production and Logistics Organization (NPLO) and NATO industrial advisory group (NIAG) recurring visits. NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies that are participating in a NPLO or NIAG contract or program. The NATO management office or agency responsible for the NPLO program will prepare a list of the government and contractor facilities participating in the program. For NIAG programs, the list will be prepared by the responsible NATO staff element. The list will be forwarded to the appropriate clearance agency of the participating nations, which will forward it to E-volve Technology Systems.
* Visitor record. E-volve Technology Systems will maintain a record of NATO visits including those by U.S. personnel assigned to NATO. The records will be maintained for three years.

# Special Security Requirements

## Critical Nuclear Weapon Design Information

E-volve Technology Systems currently has or may have special requirements for protection of Critical Nuclear Weapon Design Information (CNWDI) in the future. If CNWDI requirements exist, E-volve Technology Systems will implement procedures and comply with 32 CFR §117.20 as described in the following subsections.

### Briefings

Prior to having access to CNWDI, E-volve Technology Systems employees will be briefed on its sensitivity by the FSO or his or her alternate. The FSO will be initially briefed by a USG representative.

(1) The briefing will include:

1. The definition of CNWDI.
2. A reminder of the extreme sensitivity of the information.
3. An explanation of the individual's continuing responsibility for properly safeguarding CNWDI and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a need- to-know for the information.

(2) The briefing will also be tailored to cover any special local requirements. Upon termination of access to CNWDI, the employee will be given an oral debriefing.

### Subcontractors

E-volve Technology Systems will not disclose CNWDI to subcontractors without the prior written approval of the GCA. This approval may be included in a contract security classification specification, or equivalent, other contract-related document, or by separate correspondence.

### Records

E-volve Technology Systems will annotate CNWDI access in the CSA-designated database for all employees who have been authorized access to CNWDI.

## COMSEC

E-volve Technology Systems currently has or may have special requirements for the protection of COMSEC in the future. If COMSEC requirements exist, E-volve Technology Systems will implement procedures and comply with the following 32 CFR §117.21 requirements.

### Clearance and Access Requirements.

Before a COMSEC account can be established and E-volve Technology Systems may receive or possess COMSEC material accountable to a Contract Officer Representative (COR), individuals occupying the positions of FSO, COMSEC account manager, and alternate COMSEC account manager must have a final PCL appropriate for the material to be held in the account.

* COMSEC account managers and alternate COMSEC account managers having access to operational TS keying material marked as CRYPTO must have a final TS security clearance based upon a current investigation of a scope that meets or exceeds that necessary for the access required.
* This requirement does not apply to contractors using only data transfer devices and seed key.

Before disclosure of COMSEC information to E-volve Technology Systems, GCAs must first verify with the CSA that appropriate COMSEC procedures are in place at the E-volve Technology Systems’ facility. If procedures are not in place, the GCA will provide a written request and justification to the CSA to establish COMSEC procedures and a COMSEC account, if appropriate, at the facility and to conduct the initial COMSEC or cryptographic access briefings for the FSO and COMSEC account personnel.

Access to COMSEC information by a contractor requires a final entity eligibility determination and a USG-issued final PCL at the appropriate level; however, an Interim Top Secret entity eligibility determination or PCL is valid for access to COMSEC at the Secret and Confidential levels.

If a COMSEC account is required, the Contract Security Classification Specification, or equivalent, will contain a statement regarding the establishment of a COMSEC account as appropriate.

### COMSEC Briefing and Debriefing

All E-volve Technology Systems employees who require access to classified COMSEC information in the performance of their duties will be briefed before access is granted. Depending on the nature of COMSEC access required, either a COMSEC briefing, or a cryptographic access briefing will be given.

The FSO, the COMSEC account manager, and the alternate COMSEC account manager will be briefed by a USG representative or their designee. Other contractor employees will be briefed by the FSO, the COMSEC account personnel, or another individual designated by the FSO. The purpose of the briefing is to ensure that the contractor understands:

* The unique nature of COMSEC information and its unusual sensitivity.
* The special security requirements for the handling and protection of COMSEC information.
* The penalties prescribed in 18 U.S.C. 793, 794, and 798 for disclosure of COMSEC information.

COMSEC debriefings are not required.

E-volve Technology Systems will maintain a record of all COMSEC briefings as specified by the appropriate COR.

### U.S. Classified Cryptographic Information Access Briefing and Debriefing Requirements

U.S. classified cryptographic information does not include seed key or controlled

cryptographic items.

E-volve Technology Systems 's employee may be granted access to U.S. classified cryptographic information

only if the employee:

* Is a U.S. citizen.
* Has a final USG-issued eligibility determination appropriate to the classification of the U.S. cryptographic information to be accessed.
* Has a valid need-to-know to perform duties for, or on behalf of, the USG.
* Receives a security briefing appropriate to the U.S. Classified Cryptographic Information to be accessed.
* Acknowledges the granting of access to classified information by executing Section I of Secretary of Defense (SD) Form 572, “Cryptographic Access Certification and Termination” (available at:

[SF-0572 CRYPTOGRAPHIC ACCESS CERTIFICATION AND TERMINATION (whs.mil)](https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/sd/sd0572_2020.pdf)).

* Where so directed by a USG department or agency head, acknowledges the possibility of being subject to a CI scope polygraph examination that will be administered in accordance with department or agency directives and applicable law.

An employee granted access to cryptographic information will be debriefed and execute Section II of the SD Form 572 not later than 90 days from the date access is no longer required.

E-volve Technology Systems will maintain the SD Form 572 for a minimum of five years following the debriefing.

Cryptographic access briefings must fully meet the requirements in Section 19.2.3.

### Subcontracting COMSEC work

Subcontracts requiring the disclosure of classified COMSEC information will be awarded only upon the written approval of the GCA.

## DHS CCIPP

E-volve Technology Systems does *NOT* currently have special requirements for protection of Department of Homeland Security Classified Critical Infrastructure Protection Program (DHS CCIPP). In the event that future contracts require this kind of access, E-volve Technology Systems will implement procedures and comply with 32 CFR §117.22.

## Other

E-volve Technology Systems may currently have one or more of the following contract security requirements for:

* Alternative Compensatory Control Measures (ACCM)
* Special Access Program (SAP)
* Intelligence Information
* Restricted Data (RD)
* Formally Restricted Data
* Trans-classified Foreign Nuclear Information (TFNI)
* Naval Nuclear Propulsion Information (NNPI)

E-volve Technology Systems has included details for protecting Intelligence Information, RD, FRD, and TRNI since we either currently have or are expected to have contract security requirements for protecting these categories of information.

### Intelligence Information

National intelligence is under the jurisdiction and control of the DNI, who establishes security policy for the protection of national intelligence and intelligence sources, methods, and activities. In addition to the guidance in this rule, contractors will follow Intelligence Community directives, policy guidance, standards, and specifications for the protection of classified national intelligence and SCI.

### Restricted Data, Formally Restricted Data, and Trans-classified Foreign Nuclear Information

This section describes some of the requirements for nuclear-related information designated RD, FRD, or TFNI in accordance with the AEA and 10 CFR part 1045. 10 CFR part 1045 contains the full requirements for classification and declassification of RD, FRD, and TFNI. Information on safeguarding of RD by access permittees is contained in 10 CFR part 1016. All persons with access to RD and FRD must receive initial and periodic refresher training as required under§1045.120 10 CFR. The training must include the following information:

* What information is potentially RD and FRD.
* Matter that potentially contains RD or FRD must be reviewed by an RD derivative classifier to determine whether it is RD or FRD.
* The DOE must review matter that potentially contains RD or TFNI for public release and DOE or DoD must review matter that potentially contains FRD for public release.
* RD derivative classification authority is required to classify or upgrade matter containing RD or FRD, or to downgrade the level of matter containing RD or FRD.
* Only a person trained in accordance with §1045.120 10 CFR may classify matter containing TFNI.
* Matter containing RD, FRD, and TFNI is not automatically declassified, and only DOE-authorized persons may downgrade the category or declassify matter marked as containing RD. Only DOE or DoD authorized persons may downgrade the category or declassify matter marked as containing FRD.
* How to submit a challenge if they believe RD, FRD, or TFNI information (e.g., a guide topic) or matter containing RD, FRD, or TFNI is not properly classified.
* Access requirements for matter marked as containing RD or FRD.

All persons with access to TFNI must receive initial and periodic refresher training as required under §1045.120 10 CFR. This training may be combined with the training for access to RD and FRD. The training must include the following information:

* What information is potentially TFNI.
* Only a person with appropriate training may determine if the matter contains TFNI.
* Marking requirements for matter containing TFNI.
* Matter containing TFNI is not automatically declassified and only DOE authorized persons may downgrade the category or declassify matter marked as containing TFNI.

How to submit a challenge if they believe TFNI information (e.g., a guide topic) or matter containing TFNI is not properly classified.

### Naval Nuclear Propulsion Program

NNPI is information associated with the Naval Nuclear Propulsion Program and is governed by Office of the Chief of Naval Operations Instruction (OPNAVINST) N9210.3, “Safeguarding of Naval Nuclear Propulsion Information” (Unclassified version available at:

[SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION (NNPI) (navy.mil)](https://www.secnav.navy.mil/doni/Directives/09000%20General%20Ship%20Design%20and%20Support/09-200%20Propulsion%20Plants%20Support/N9210.3%20(Unclas%20Portion).pdf#search=N9210%2E3)

Naval Reactors, a joint DOE/Department of Navy organization established under 50 U.S.C. 2406 and 2511, is responsible for the protection of this information. All contracts which grant access to NNPI must require compliance with the specific safeguarding requirements contained in OPNAVINST N9210.3. All waivers or deviations involving security requirements protecting NNPI require Naval Reactors' concurrence. Classified NNPI may not be processed on a E-volve Technology Systems information system unless approved by the cognizant authorizing authority with concurrence from Naval Reactors.

If future contracts require any additional accesses, E-volve Technology Systems will implement procedures and comply with 32 CFR §117.23.

# Emergency Procedures

## 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 to secure classified information. For example, in the 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. E-volve Technology Systems will report to DCSA any emergency that renders their location incapable of safeguarding classified material as soon as possible.

## Emergency Contact Numbers

|  |  |
| --- | --- |
| Name | Phone Number |
| FSO: Tanya Johnson | 240-724-0104 |
| SMO: Diedre Boone |  |
| ITPSO: Tanya Johnson | 240-724-0104 |
| GCA |  |
| Prime Contractor |  |
| DCSA: NAESOC | 888-282-7682 (Option #7) |
|  |  |

# Definitions

|  |  |
| --- | --- |
| 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 unauth4orized disclosure in the interest of national security. |
| Cleared Employees | All E-volve Technology Systems 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 Part §117, the NISPOM Rule for safeguarding classified information that, because of its size, nature, and operational necessity, cannot be adequately protected by the normal safeguards, or stored during nonworking hours in approved containers. |
| 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  Covered Individual | Classified information or material that requires protection whereby unauthorized disclosure could reasonably be expected to cause damage to our national security.  All persons who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees. |
| Controlled Unclassified Information (CUI) | CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government wide policies. |
| 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. |
| Personally Identifiable Information (PII) | PII is any information that can be used to distinguish or trace a person's identity either alone or when combined with other information that is unique. |
| 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 Part 117, the 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 Part 117, the NISPOM Rule for the contractor’s operations and involvement with classified information at the contractor’s facility. |
| Subcontractor | A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor. |
| Top Secret | Classified information or material that requires the highest degree of protection, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to our national security. |
| Unauthorized Person | A person not authorized to have access to specific classified information in accordance with the requirements of the 32 CFR Part 117 NISPOM Rule. |

# Abbreviations and Acronyms

|  |  |
| --- | --- |
|  |  |
| ACCM | Alternative Compensatory Control Measures |
| AFSO | Assistant Facility Security Officer |
| AIS | Automated Information System |
| ATOMAL | NATO Marking for U.S. Atomic Information |
| C | Confidential |
| CAGE  CDC | Commercial and Government Entity  Cleared Defense Contractor |
| CE | Continuous Evaluation |
| CFR | Code of Federal Regulations |
| CI | Counterintelligence |
| CISA | Counterintelligence Special Agent |
| COMSEC | Communication Security |
| CSA | Cognizant Security Agency |
| CSO | Cognizant Security Office |
| CSR | Customer Service Request |
| CUI | Controlled Unclassified Information |
| DHS CCIPP | Department of Homeland Security Classified Critical Infrastructure Protection Program |
| DNI | Director of National Intelligence |
| DoD | Department of Defense |
| DoD CAS | Department of Defense Consolidated Adjudications Services |
| DOE | Department of Energy |
| DCSA | Defense Counterintelligence and Security Agency |
| DISS | Defense Information System for Security |
| DTIC | Defense Technical Information Center |
| e-APP | NBIS Electronic Application |
| e-QIP | Electronic Questionnaires for Investigation Processing |
| FBI | Federal Bureau of Investigation |
| FCL | Facility (Security) Clearance |
| FOCI | Foreign Ownership, Control, or Influence |
| FRD | Formally Restricted Data |
| FSO | Facility Security Officer |
| GCA | Government Contracting Activity |
| GSA | General Services Administration |
| ISOO | Information Security Oversight Office |
| ISR | Industrial Security Representative |
| ISSM | Information System Security Manager |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| ITPSO | Insider Threat Program Senior Official |
| KMP | Key Management Personnel |
| NBIS | National Background Investigation Services |
| NCSC | National Counterintelligence and Security Center |
| NDA | Nondisclosure Agreement |
| NISP | National Industrial Security Program |
| NISPOM | National Industrial Security Program Operating Manual |
| NISS | National Industrial Security System |
| NNPI | Naval Nuclear Propulsion Information |
| NTK | Need-to-Know |
| OPM | Office of Personnel Management |
| PCL | Personnel Security Clearance |
| PII | Personally Identifiable Information |
| POC | Point of Contact |
| PR | Periodic Reinvestigation |
| PSMO-I | Personnel Security Management Office for Industry |
| RD | Restricted Data |
| S | Secret |
| SAP | Special Access Program |
| SCG | Security Classification Guide |
| SCI | Sensitive Compartmented Information |
| SEAD | Security Executive Agent Directive |
| SF | Standard Form |
| SMO | Senior Management Official |
| SMS | Text Message Capabilities |
| SPP | Standard Practice Procedures |
| SR | Security Review |
| TFNI | Trans-classified Foreign Nuclear Information |
| TS | Top Secret |
| U | Unclassified |
| UD | Unauthorized Disclosure |
| U.S. | United States |
| USG | United States Government |

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
| 1.0 | 7/19/2018 | e-Volve Technology Systems, Inc. | Baseline version associated with Top Secret FCL and no safeguarding |
| 2.0 | 8/24/2023 | Security Consulting Group, Inc. | Changes to complete document. Review entire SPP |
|  |  |  |  |
|  |  |  |  |

# Appendix A **–** SEAD 3 Reporting Matrix and Forms

|  |  |  |  |
| --- | --- | --- | --- |
| **Reportable Activity** | **Secret and “L”** | **Top Secret and “Q”** | **Reporting Form Attachment #** |
| Alcohol- and Drug-Related Treatment | Yes | Yes | 19 |
| Application for, Possession, or Use of a Foreign Passport or Identity Card for Travel | Yes | Yes | 8-9-10 |
| Arrests | Yes | Yes | 15 |
| Attempted Elicitation, Exploitation, Blackmail, Coercion, or Enticement | Yes | Yes | 13 |
| Bankruptcy or Over 120 Days Delinquent on Any Debt | Yes | Yes | 16 |
| Continuing Association with a Known Foreign National(s) or Foreign National Roommate(s) | Yes | Yes | 3 |
| Cryptocurrency Ownership | Yes | Yes | 20 |
| Foreign Citizenship | Yes | Yes | 7 |
| Foreign Travel | Yes | Yes | 1 |
| Media Contacts | Yes | Yes | 14 |
| Reportable Actions by Others | Yes | Yes | 21 |
| Unofficial Contact with a Known or Suspected Foreign Intelligence Entity | Yes | Yes | 2 |
| Adoption of Non-U.S. Citizen Children | No | Yes | 12 |
| Cohabitant(s) | No | Yes | 17 |
| Financial Issues and Anomalies:  Including, but not limited to, garnishment; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain | No | Yes | 16 |
| Foreign Bank Account | No | Yes | 5 |
| Involvement in Foreign Business | No | Yes | 4 |
| Marriage | No | Yes | 18 |
| Ownership of Foreign Property | No | Yes | 6 |
| Voting in a Foreign Election | No | Yes | 11 |

|  |  |  |
| --- | --- | --- |
| 01 | Foreign Travel |  |
| 02 | Foreign Contacts Intelligence Entity |  |
| 03 | Foreign Contacts |  |
| 04 | Foreign Activities: Involvement in Foreign Business |  |
| 05 | Foreign Activities: Foreign Bank Account |  |
| 06 | Foreign Activities: Ownership of Foreign Property |  |
| 07 | Foreign Activities: Foreign Citizenship |  |
| 08-09-10 | Foreign Activities: Foreign Passport/Identity Card |  |
| 11 | Foreign Activities: Voting in a Foreign Election |  |
| 12 | Adoption of a Non-US Citizen Child(ren) |  |
| 13 | Attempted Elicitation, Exploitation, Blackmail, Coercion, Enticement |  |
| 14 | Media Contacts |  |
| 15 | Arrests |  |
| 16 | Financial Issues or Anomalies |  |
| 17 | Cohabitation |  |
| 18 | Marriage |  |
| 19 | Alcohol and/or Drug-Related Treatment |  |
| 20 | Cryptocurrency |  |
| 21 | Reportable Actions by Others |  |