STANDARD PRACTICE PROCEDURES (SPP)
MANUAL

1211 N. West Shore, Ste.
410
Tampa, FL 33607

NOTE: The chapter, section, and paragraph references of this SPP correlate directly with the NISPOM. However, only NISPOM paragraphs that require comments or supplement are addressed. The Insider Threat Program (ITP) is addressed in our 9Line ITP.

TABLE OF CONTENTS

CHAPTER 1 GENERAL PROVISONS AND REQUIREMENTS

Section 1. Introduction

1-100 Purpose 5
1-101 Authority 5

Section 2. General Requirements

1-200 General Requirements 6
1-201 Facility Security Officer (FSO) 6
1-202 Insider Threat Program).....6
1-205 Cooperation with Federal Agencies and Official Credentialed Representatives ofthose agencies 6
1-206 Security Trainings and Briefings.....6
1-207 Security Reviews 7
1-208 Hotlines.....7

Section 3. ReportingRequirements

1-300 Reporting Requirements 8
1-301 Reports to be submitted to the FBI 8
1-302 Reports to be submitted to the CSA.....8
1-303 Reports of Loss, Compromise, or Suspected Compromise.....8
1-303a-b Preliminary Inquiry / Initial Report 10
1-303 c Final Report.....11
1-304 Individual Culpability Report 12

CHAPTER 2 SECURITY CLEARANCES

Section 1. Facility Clearances

2-100 General.....12
2-110 Termination of FCL 12

Section 2. Personnel Security Clearances

2-200 General.....12
2-203 Common Adjudicative Standards 12
2-212 Consultants 13

Section 3. Foreign Ownership, Control, or Influence (FOCI)

2-300 Policy.....13

CHAPTER 3 SECURITY TRAINING AND BRIEFINGS

Section 1. Security Training and Briefings

3-102 FSO Training.....13
3-104 Government- Provided Briefings..... 14
3-107 Initial Security Briefing.....14
3-108 Refresher Training..... 14
Additional Briefings 14
Foreign Travel Briefings..... 14
3-109 Debriefings.....15

CHAPTER 4 CLASSIFICATION AND MARKING.....15

CHAPTER 5 SAFEGUARDING CLASSIFIED INFORMATION 15

Section 1. General Safeguarding Requirements

5-101 Safeguarding Oral Discussions..... 15
5-102 End of Day Security Checks 15
5-511 Disclosure to the Public..... 15
5-700. Disposition and Retention..... 15

CHAPTER 6 VISITS AND MEETINGS

Section 1. Visits

6-101 Classified Visits 16
6-105 Long-Term Visitors.....16

Section 2. Meetings
6-200 General..... 16
6-203 Request to Attend Classified Meetings.....16

CHAPTER 7 SUBCONTRACTING

Section 1. Prime Contractor Responsibilities

7-100 General..... 17

CHAPTER 8 IS Security 17

CHAPTER 9 SPECIAL REQUIREMENTS 18

CHAPTER 10 INTERNATIONAL SECURITY REQUIREMENTS 18

Section 7. NATO Information Security Requirement.....18

General 18

Classification Levels.....18
NATO Restricted 18
NATO Contracts 19
NATO Facility Security Clearance Certificate..... 19
PCL Requirements.....19
NATO Briefings.....19
10-708 Subcontracting for NATO Contracts 19
10-710 Classification Guidance 19

CHAPTER 11 MISCELLANEOUS INFORMATION 20

9LINE ADDITIONS TO THE SPP.....20

9LINE ACKNOWLEGMENT OF SPP REVIEW..... 27

CHAPTER 1
General Provisions and Requirements

1-100. Purpose. This document is intended to provide 9Line, LLC (9Line) employees with security policies, procedures, and guidance applicable to the implementation of the requirements, restrictions and other safeguards contained in the National Industrial Security Program Operating Manual (NISPOM). This SPP is intended for use by the Facility Security Officer (FSO) and Assistant Facility Security Officers (AFSOs) as well as 9Line Leadership and Employees. Additional security procedures and awareness materials for cleared employees will be published and distributed separately. There may be additional policies, procedures, and guidance provided by the client of which 9Line employees will be responsible for along with this SPP.

Waivers, Exceptions, Modifications, Additions, and/or deletions to this SPP will be provided to the 9Line FSO. The employee shall specify requests, in writing, accordingly.

The 9Line office located at 1211 N. West Shore, Ste. 410, Tampa, Fl 33607 (Cage Code: 5FTW3) and maintains a TOP SECRET facility clearance granted by the Defense Counterintelligence and Security Agency (DCSA).

All 9Line employees and consultants are provided security briefings and instruction and may be required to read and understand this SPP and are ultimately responsible for complying with all security procedures defined within this document. Any deviation from this SPP as stated herein must be approved by the Facility Security Officer (FSO) and appropriate Program Manager (PM) prior to implementation.

1-101. Authority. The security procedures contained herein are in accordance with applicable 9Line security policies and procedures and encompass the customer's security procedures as required. The procedures also include security requirements outlined in the Department of Defense National Industrial Security Program Operating Manual (NISPOM) dated February 28, 2006, with Change 2 incorporated May 18th, 2016, as well as all applicable Industrial Security Letters and all applicable Director of Central Intelligence Directives (DCIDs).

Security Organization

9Line employs a mature, integrated approach to management and oversight of the industrial security operation at all levels of the company. The 9Line FSO sets basic policy and provides the leadership and guidance necessary to integrate all security initiatives and is ultimately responsible for ensuring the execution of a sound, compliant security program that protects our customers' classified information.

9Line has one AFSO who is organized and dedicated to developing and implementing common security programs comprised of policies, procedures, metrics, training, and self-

inspections. These programs are designed to manage the implementation of the following key industrial security processes:

- Personnel Security
- Investigation
- Information Security
- Information Assurance
- Physical Security
- Crisis Management
- Insider Threat
- Protective Services
- Emergency Preparedness
- International Security
- Security Awareness, Training, and Education
- Operations Security

1-200. General Requirements. 9Line employees located on federal installations will be expected to follow the host installation procedures in addition to following 9Line policies and procedures with respect to safeguarding classified information.

1-201. Facility Security Officer (FSO). The FSO at the 9Line facility at 500 N Westshore Blvd Ste 405, Tampa, FL 33609 is Scott Heintz, also the President, CEO and owner and sole Key Management Personnel (KMP). He will implement applicable requirements of the NISPOM and related Federal requirements for classified information. As required in Chapter 3 of the NISPOM, Mr. Heintz has completed the requisite training to perform his duties as FSO. Any plans to either replace or reassign the FSO will be immediately reported to the DSS ISR assigned to 9Line. 9Line has one Assistant FSO, Mr. David Heintz, who is FSO trained and qualified and will support the 9Line Industrial Security Program (ISP) requirements for the company and the FSO.

1-202. Insider Threat Program. 9Line ITP is provided under separate cover.

1-204. Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies. 9Line will cooperate fully with Federal agencies and their officially credentialed representatives during official inspections and investigations concerning the protection of classified information, and during personnel security investigations of present or former employees and others.

1-206. Security Trainings and Briefings. 9Line is responsible for advising all cleared employees, including those outside the United States, of their individual responsibility for safeguarding classified information. 9Line will provide training as appropriate, according to chapter 3, to cleared employees by initial briefings, refresher briefings, and debriefings. 9Line also provides all required training to uncleared employees to enable more awareness and have a stronger security program.

1-207. Security Reviews

Government Reviews. 9Line will cooperate and participate in periodic security reviews to ensure that required safeguards are in place for the protection of classified information.

Contractor Reviews. The conduct of formal self-inspections and reviews of the 9Line facility will be performed at intervals consistent with risk management principals. As a minimum, a formal internal evaluation should occur at least once per year, but also following any major or significant changes in the level, volume, or nature of classified activity.

1-208. Hotlines. All 9Line employees will be provided the numbers for the federal agency hotlines. Additionally, hotline posters will be posted throughout the facility.

Defense Hotline
The Pentagon
Washington, DC 20301-1900

Office of the Inspector General
1000 Independence Avenue, SW
Room 5A235 800-424-9098
Washington, DC 20585
202-586-4073
800-541-1625

DOE Hotline
Department of Energy
NRC Hotline
U.S. Nuclear Regulatory Commission
Office of the Inspector General
Mail Stop TSD 28
Washington, DC 20555-0001
800-233-3497

CIA Hotline
Office of the Inspector General
Central Intelligence Agency
Washington, DC 20505
703-874-2600

1-300. Reporting Requirements. The 9Line office coordinates and/or effects the notification to cognizant government security offices regarding any/all changed conditions affecting 9Line. This includes changes to the DD Form 441 and SF 328, local facility KMPs and changes thereto, changes in address, storage capabilities, adverse information reporting, and any company-wide changes which may affect this security program.

1-301. Reports to be submitted to the FBI. Immediate notification will be made to the FBI and 9Line Security concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at this location. Initial reports would be made by phone but then followed up in writing to the company FSO who will submit a copy to the CSA. DCSA counterintelligence POC for our area will also be notified.

1-302. Reports to be submitted to the CSA. The FSO is responsible for prompt and accurate reporting and will ensure the following reports will be submitted to the CSA and 9Line Security in accordance with NISPOM 1-302:

- Adverse Information
- Suspicious Contacts
- Change in Cleared Employee Status
- Citizenship by Naturalization
- Employees Desiring Not to Perform on Classified Work
- Standard Form (SF) 312
- Change Conditions Affecting the Facility, including change in ownership, operating name, or address, change in key management personnel, action to terminate business, any change concerning foreign ownership, control, or influence
- Changes in Storage Capability
- Inability to Safeguard Classified Material
- Security Equipment Vulnerabilities
- Unauthorized Receipt of Classified Material
- Employee Information in Compromise Cases
- Disposition of Classified Material Terminated from Accountability
- Foreign Classified Contracts

1-303. Reports of Loss, Compromise, or Suspected Compromise. 9Line is legally and contractually obligated to protect classified information from unauthorized disclosure. 9Line will maintain an adequate security program to assist management and technical staff in their responsibilities in the proper handling of classified material and information. Improper actions that jeopardize classified information will be reported to the 9Line FSO to investigate and, where applicable, report to the appropriate government authority. The following provides guidelines to 9Line management for the administration of corporate policy as it relates to security violations or procedural infractions by employees and consultants.

- **Management Responsibilities.** At 9Line, it is the responsibility of all levels of management to ensure that an adequate security program is established, carried out and encouraged at its facility. It is also management's responsibility to ensure that the FSO monitors the security program for compliance and investigates violations of security. Senior Management is responsible for imposing administrative remedies that are appropriate to the severity of any infraction or violation, and as set forth in this section.
- **Disciplinary Action Policy.** Disciplinary action taken by 9Line will be based upon a review of each case's own merits. The seriousness of the violation will be determined by whether a compromise, suspected compromise, or loss of classified information has occurred, or if it was only administrative in nature. Additional factors for consideration will be employee negligence, and previous violations. 9Line disciplinary action may be anyone or a combination of the following, depending upon the above factions:
    - Regardless of the security infraction, refresher training will be provided to ensure the employee understands the security procedures and practices to prevent future security violations.
    - Disciplinary letter signed by the Facility Security Officer placed in the employees personnel file.
    - Written notification to the Facility Supervisor concerning at fault employees lack of ability to protect classified information in accordance with security classification guides, the NISPOM, and 9Line Security Policies.
    - Recommendation to DCSA through the CSA for suspension of concerned employee's access to classified information pending further inquiry
    - Recommendation to DSCA through the CSO for revocation of concerned employee's clearance. A written recommendation to the appropriate 9Line Manager to terminate employment of the concerned employee.

  A graduated scale of disciplinary actions is provided on page 24 of this document as part of the 9Line additions to the SPP.

- **Individual Responsibilities.** Employees are responsible for the proper protection of classified information. They must be familiar with and comply with the security guidance provided by all security guidelines set forth by this SPP.

- **Definition of Terms.** To ensure equal application of the 9Line Security Violation Policy throughout the corporation, following are some definitions of terms used in this section, which may be helpful:
    - Compromise: The disclosure of classified information to persons not authorized access to it.
    - Suspected Compromise: An instance of loss of control or safeguarding of classified information or material where the facts determine that the opportunity or probability exists for disclosure to unauthorized person(s) but is not confirmed as actual.

- Potential Compromise: An instance of loss of control or safeguarding of classified material or information where there is no evidence that the information could have been disclosed to unauthorized personnel.
- Security Infraction: A failure on the part of an individual to follow or comply with a security policy, practice or procedure as outlined in the NISPOM or this SPP, when the investigation indicates that the infraction did not involve actual, suspected, or potential compromise of classified information or material.

- **Internal Reporting Procedures.** The reporting of security infractions or violations is absolutely essential in order to minimize the extent of actual or potential compromise. Prompt action in the case of an infraction may prevent compromise of the material or information involved.

- **Responsibility to Report.** All employees shall be briefed on their individual responsibility to report security infractions or violations promptly to the FS or AFSOs.

- **Facility Security Officer Responsibility.** Upon report of a security violation or procedural infraction, the FSO shall:
  - Make an initial determination of the nature of the incident
  - Take appropriate action to safeguard the affected material
  - Investigate and report the findings of the investigation to the appropriate manager.
  - Make any formal reports to government agencies, as may be required, including initial and follow-up investigative reports and adverse information report
  - Take action as appropriate with the employee

1-303a-b. Preliminary Inquiry/Initial Report. Upon review of the incident and coordination with line management, the FSO may need to check records, review the SPP, examine material evidence, and interview persons having direct knowledge of the facts on the incident. The following information is required in the preliminary inquiry:

- What is alleged to have happened, where, and when did the violation occur?
- Who reported the violation, to whom, and when?
- What classified information was involved? (Attach a list of the classified material, if appropriate and cite the authority for possession.)
- What was the classification of the information involved?
- Who are the originators of the information involved? Identify the procuring activity.
- When, for how long, and under what circumstances was classified information vulnerable to unauthorized disclosure? Determine identity of unauthorized persons likely to have had access to the information.

- What actions were taken to secure the classified information and/or limit the damage before the inquiry began, and when and by whom were they taken (inventories, securing of material, changing of combinations and so forth)?
- Is any classified material lost or unaccounted for? (In the event of a loss, a thorough search shall be conducted for the classified material.)

If the preliminary inquiry confirms that a loss, compromise, or suspected compromise of classified information occurred, or that a security violation involving COMSEC, NATO, or foreign government information occurred, an initial report of the incident shall be immediately reported (normally within 24 hours of the incident) to the CSO. Submission of the initial report shall not be deferred pending completion of the entire investigation. After submission of the initial report, a complete investigation of the incident, unless otherwise notified by the DCSA/CSO will be conducted. In the event the preliminary inquiry does not confirm a violation that requires a report to the DCSA/CSO, the results shall be retained for review during the next scheduled inspection by the DCSA/CSO. These "internal reports" should be placed into the personnel security files of any employee determined to be responsible/culpable for the violation. If a deliberate and willful disregard for security procedures and/or a known loss or compromise of classified material is immediately determined, telephonic notification should be made of the incident to the local DCSA office.

Review and Appeal Procedures. After the investigation is accomplished and prior to the imposition of corrective action and discipline, and the final report submitted to the DCSA/CSO, the findings of the incident will be reviewed as outlined in 9Line SPP.

1-303c. Final Report. When the preliminary investigation reveals a compromise, suspected compromise or that compromise cannot be precluded, a final investigation and report shall be submitted within 15 working days of the initial report. If delays in completing either the investigation or final report occur, a telephonic request for extension should be requested of the local DCSA Field Office. The final report/Administrative Inquiry (AI) should as a minimum answer the following questions:

- Any of the information required for the preliminary inquiry not included in the initial report;
- The name, position, social security number, date and place of birth, and date of the clearance of the individual(s) who was primarily responsible for the incident, including a record of prior loss, compromise, suspected compromise, or security violation for which the individual had been determined responsible;
- A statement of the corrective action taken to preclude a recurrence of similar incidents and the disciplinary action taken against the responsible individual(s), if any;
- Specific reasons for reaching the conclusion that: (i) loss or compromise occurred, (ii) compromise is suspected, (iii) the probability of compromise is considered remote, or (iv) compromise did not occur. (See attached flow chart for guidance -Probability of Compromise Determination)

- Was the SPP adequate? If not, specify inadequacies. Who was responsible for the inadequacy?
- Why did the violation occur?
- If the violation occurred outside the facility, were the reporting requirements of the NISPOM complied with? If not, why not. If so, when and to whom was the report made?
- Recommend administrative actions based on 9Line graduated sale of disciplinary actions.

3-304. Individual Culpability Reports. 9Line accepts its responsibility to keep the government (DCSA) informed when cleared personnel have been identified as culpable for a security violation provided that one or more of the following facts are evident:

- The violation involved a deliberate disregard of security requirements.
- The violation involved gross negligence in the handling of classified material.
- The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness, such as, two or more violations in a 12-month period.

If a report was already submitted as either an adverse information report or an initial or final report citing the culpable individual, a separate report to DCSA is not required.

CHAPTER 2
Security Clearances

2-100. General - Facility Security Clearances. 9Line has a Facility Clearance (FCL) at the TOP SECRET level. All facility Key Management Personnel (KMP), senior facility officials and the FSO, are designated qualified persons who are responsible for security management at this facility and maintain TOP SECRET clearances. A list of the KMPs is kept current by the FSO and any changes are submitted via the NISS/DISS to DCSA.

2-110. Termination of FCL. If the FCL is terminated for any reason, all classified material will be returned to the appropriate GCA or disposed of as instructed by the CSA.

2-200. General - Personnel Security Clearances. All Personnel Security Clearances (PCLs) for the 9Line facility are processed and maintained 9Line's corporate security office. The FSO and AFSO for the 9Line facility is responsible for requesting the clearances, assisting the individuals with the EQIP process and e-fingerprints or cards, as well as provide security briefings and submit visit requests.

2-203. Common Adjudicative Standards. It is a 9Line policy that employees nominated for a security clearance shall have an opportunity to understand the adjudication criteria by which they will be screened and if any supplemental screening measures, such as background checks, drug testing or polygraph, are anticipated prior to having their names submitted for government processing.

- **Clearance Reinstatements.** Clearances may be reinstated upon verification of the clearance record within the JPAS system. If the individual is not found in the JPAS system, the security person must execute an RRU (Request for Research Upgrade) within the DISS/JPAS systems.
- **Individual Right Of Privacy.** 9Line accepts an important responsibility to employees in nominating an individual for a security clearance and understands that in doing so the FSO is exposed to detailed personal information for the individual. The FSO understands that information is provided for the sole purpose of providing the government with the background information it needs to make a clearance decision (adjudication). This data may not be collected for any other purpose. All personal data supplied by employees or consultants is considered as privileged information and shall be handled at all times in a manner consistent with the protection of the right of privacy of each individual. Access to this data shall be limited to those employees who directly participate in the clearance processing procedures. Employees, Consultants, or Subcontractor personnel security files shall be maintained in a lockable filing cabinet in order to prohibit unauthorized access to this information. If maintained electronically, the files will be maintained in such a manner that access by unauthorized persons do not have access (Le., encrypted, password protected, etc.).
- **"Privacy Portion" Processing.** Personnel who are responsible for processing security applications on SF 86, or similar forms used by other agencies, shall advise applicants prior to processing that if they have a significant personal matter which they desire not to disclose to 9Line, they may request an interview with the appropriate U.S. Government representative rather than completing that item in the Privacy Portion. Alternatively, the individual may complete a detailed statement, which is to be sealed by the individual in an envelope and marked as an attachment to the clearance application. The FSO will mail the sealed statement to the appropriate agency for review.

2-212. Consultants. As individuals under contract to provide professional or technical assistance to 9Line, many consultants may require access to classified information. It is understood that the consultant may only access classified material away from the 9Line facility in connection with an authorized visit or if employed at a customer designated location. A consultant agreement between 9Line and the consultant will be in place prior to access and the agreement will set forth the respective security responsibilities.

2-300. Foreign Ownership, Control, or Influence (FOCI). The SF328 for 9Line is prepared, submitted, and maintained for review. Copies of the most recent FOCI certification may be obtained from the ESSS office. 9Line will notify DCSA if there are any changes to the SF328.

CHAPTER 3
Security Training and Briefings

Fundamental to successful and effective security programs is the awareness and motivation of the employees who participate in the program. A basic tenet of the NISP is that cleared individuals are both accountable and responsible for carrying out their security duties. 9Line policy is that each employee, consultant, or affiliate with access to 9Line premises will be afforded a series of security awareness briefings dependent on their level of access, clearance, and/or duties. It also provides a variety of security information, sample briefings, and useful references to assist in security awareness efforts.

3-102. FSO Training. 9Line is responsible for ensuring that the FSO, and others performing security duties, complete training considered appropriate by the CSA. Requirements shall be based on the facility's involvement with classified information. Training should be completed within 1 year of appointment to the position of FSO.

3-104. Government Provided Briefings. The CSA is responsible for providing initial security briefings to the FSO and for ensuring that the other briefings required for special categories of information are provided.

3-107. Initial Security Briefings. When a 9Line employee or Consultant is granted a security clearance, he or she must be afforded a personal (or group) briefing prior to accessing any classified information and material. 9Line provides this Initial Security Briefing in both electronic and hard copy form and as outlined in paragraph 3-106 of the NISPOM, includes the following:

- Threat Awareness
- Defense Security Briefing
- Overview of the Security Classification System
- Employee reporting obligations
- Security procedures and duties applicable to the employee's job
- Disciplinary Actions related to Security Violations
- Insider Threat Program

3-108. Refresher Briefings. All cleared employees and consultants will receive security education on at least an annual basis. 9Line has an Annual Security Refresher Briefing that reinforces the information in the Initial Security Briefing and is made available to all employees and consultants, either in electronic or hard copy form.

Additional Briefings. In addition to the Initial Security Briefing, all cleared employees and consultants will receive required Annual Refresher briefings and other briefings depending on their circumstances (i.e., NATO, COMSEC, OPSEC, Reporting Requirements, Threat

Briefings, etc.) as required by the NISPOM and other government directives. This includes the Insider Threat Program training.

Foreign Travel Briefings. The 9Line Security Office will provide foreign travel briefings commensurate with the employee traveling, reason for traveling, and location of travel. All foreign travel, whether business or personal, shall be reported by 9Line personnel regardless of their clearance eligibility/access level at least 30 days prior (unless it is unexpected travel) so that an appropriate briefing can be provided to the employee.

3-109. Debriefings. When an employee or consultant clearance is to be terminated because of layoff, termination of employment, non-renewal of consulting agreement, or when the employee no longer requires access to classified information (administrative termination), it is necessary to provide a debriefing. The person being debriefed shall be reminded of his/her obligation to continue to protect classified information from unauthorized disclosure, and that he/she understands the sanctions set forth in the Extracts of Espionage and Sabotage. The individual's record will be annotated in JPAS to record the administrative termination of the clearance. All unexpired Classified Visit Requests must be canceled as soon as possible. The employee security file shall be retained for government inspection for at least two years.

CHAPTER 4
Classification and Marking

9Line does not currently have classified storage therefore it does not participate in derivative classification and/or marking responsibilities at the company facility. Employees who participate in derivative classification and/or marking at the client site shall follow the guidelines provided by the site security manager and the security classification guide provided for that particular program.

CHAPTER 5
Safeguarding Classified Information

5-101. Safeguarding Oral Discussion. 9Line employees shall be aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or places, or in any manner that permits interception by unauthorized persons. Additionally, they should be careful not to disclose unclassified information which may be deemed export controlled to foreign nationals.

5-102. End of Day Security Checks. Security checks are conducted at the end of each day or shift to ensure that all Classified (at government sites only), Proprietary and/or FOUO documents have been secured accordingly.

5-511. Disclosure to the Public. 9Line employees shall not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the DD254 for the contract or as otherwise specified by the GCA. Employees should be reminded that just because they may see information relating to a classified contract (via written, electronic, or virtual means) or hear discussions (via conversations, recordings, radios or television) does not mean that the information has been approved for release and should continue to safeguard that information until they are told by the program manager, customer or the 9Line that the information isreleasable.

5-700. Disposition and Retention. Although 9Line does not maintain classified storage at their facility, there are still many sensitive documents (bids, proposals, rates, clients, etc.) that should be safeguarded. All paper related products, regardless of the information contained on them, should be shredded to ensure that no documentation, singularly or collectively, gives away 9Line proprietary information.

CHAPTER 6
Visits and Meetings

Classified visits require that Visit Requests, as stipulated in NISPOM 6-104, are sent to the hosting facility prior to the scheduled visit -this can be accomplished either through DISS, fax, or other approved channels.

For incoming visits at the 9Line Government locations/facilities that our contractors are responsible for, all clearances will be verified in DISS and the identity of all individuals will be verified with positive identification (Company or other Photo ID Card, Driver's License with photo, etc.) official government pictured identification card. Additionally, the "need-to-know" will be determined and verified with the program manager or the employee hosting the visit.

6-101. Control of Visitors. 9Line does not store or process classified information. Additionally, the office of 9Line is such that the open floor plan allows all individuals there to be seen. Employees will be notified if there is a visitor in the office that is a foreign national.

6-105. Long-Term Visitors. When government employees or employees of one contractor are temporarily stationed at another contractor's facility, the security procedures of the host contractor will govern.

- Contractor procedures shall not require government employees to relinquish control of their work products, whether classified or not, to a contractor.
- Contractor employees at government installations shall follow the security requirements of the host. However, this does not relieve the 9Line from security oversight of their employees who are long-term visitors at governmentinstallations.

6-200. Classified Meetings. Classified discussions and/or meetings will not be held at 9Line. All classified meetings/briefings will be held at the client site.

6-203. Requests to Attend Classified Meetings. Requests for the passing of clearances for a visit will be provided to the Security Office NLT 3 days prior to travel, unless otherwise stipulated by the host facility. Requests will include:

- Names of all 9Line employees/consultants who are attending
- Name of company/facility you are visiting
- Level of clearance to be passed
- Inclusive dates of visit
- Name & contact information for the POC you are visiting
- SMO Code, Fax Number or contact information for the visiting Security Office

CHAPTER 7
Subcontracting

7-101. Prime Contractor Responsibilities. It may be necessary during the performance of a contract issued to 9Line to seek assistance from a subcontractor to effectively complete the contractual effort. Selection of subcontractors and issuance of Purchase Orders (POs) requires the coordinated effort of the Contracts Department and FSO. This coordination is essential to ensure the prospective subcontractor has an appropriate facility clearance (FCL) and safeguarding capability, and the necessary security classification guidance to properly protect and safeguard the classified information released to the subcontractor. Classification guidance is provided to the subcontractor via a Contract Security Classification Specification (DD Form 254). There is no substitute for the DD Form 254, and it must be provided as part of the subcontract for all classified procurements.

- **Determining Clearance Status of Prospective Subcontractors.** It is a mandatory requirement to verify a prospective subcontractor's facility clearance and safeguarding capability (as required) prior to releasing or allowing access to classified information by a subcontractor. This verification will be the responsibility of the 9Line FSO. Verification of facility clearance and safeguarding capability may be obtained via the Industrial Securities Facility Database (ISFD).
- **Requesting Facility Clearances for Uncleared Subcontractors.** If a prospective subcontractor does not have an appropriate facility clearance or safeguarding capability, 9Line will request the CSA of the subcontractor to initiate clearance action. Request to process a prospective subcontractor for an FCL must be based on a bona fide need for the subcontractor to have access to, or possession of, classified information. Under no circumstances will a subcontractor be allowed to have access to classified information until a facility clearance is issued.
- **Security Requirements and Processing of Subcontracts.** During all phases of a classified subcontract (e.g., Request for Proposal (RFP), Request for Quotation (RFQ), Purchase Order (PO), etc.) security classification guidance must be provided. This

includes service type subcontracts for guard services, reproduction services, engineering services, and graphic arts. It will be the responsibility of the designated Subcontract Administrator to review the proposed P.O. to determine if the subcontractor will need access to classified information and notify the 9Line FSO. Security classification guidance provided to the subcontractor will be issued via a DD Form 254. The DD Form 254 will be revised when changes in performance occur.

CHAPTER 8
Automated Information Systems

9Line does not currently possess accredited Information Systems (IS) which are needed for processing classified information. 9Line computers are not to be used for any form of classified processing. If classified processing is required, please contact the company security office.

CHAPTER 9
Special Requirements

Special Requirement accesses, such as Restricted Oata (RO), Formerly Restricted Oata (FRO), NATO, COMSEC, etc. are contract specific and designated in the DD 254 for each contract. If the accesses are required, the FSO will initially be briefed by the COR and Contracting Officer and Government ISO and will then brief those employees requiring access to ensure they are aware of their responsibilities, as set forth in Chapter 9 of the NISPOM.

CHAPTER 10
International Security Requirements

9Line has employees located in Germany and Hawaii under a classified contract and follows the contract security requirements for those locations as well as company policy. We do not have foreign classified programs or business, or any pre-contract negotiations or award of a classified contract. Additionally, the FSO will work with DCSA to ensure that all applicable federal laws, policies, rules, and regulations are strictly adhered to.

Section 7
NATO Information Security Requirements

10-700. General. This section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO (USSAN) for safeguarding NATO information provided to U.S. industry. 9Line has a NATO Secret requirement for one of our current classified contracts and follows all the requirements set forth by the government DD-254 and contract security requirements.

10-701. Classification Levels. NATO has the following levels of security classification: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and UK Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

10-702. NATO RESTRICTED. NATO RESTRICTED does not correspond to an equivalent U.S. classification. NATO RESTRICTED does not require a PCL for access. An FCL is not required if the only information to which the company will have access is NATO RESTRICTED. IS handling only NATO RESTRICTED information do not require certification or accreditation. NATO RESTRICTED information may be included in U.S. unclassified documents. The U.S. document must be marked, "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." NATO RESTRICTED material may be stored in locked filing cabinets, bookcases, desks, or other similar locked containers that will deter unauthorized access.

10-703. NATO Contracts. NATO contracts involving NATO-unique systems, programs, or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO Management Agency, the NATO Research Staff, or a NATO Command. In the case of NATO infrastructure projects (e.g., airfields, communications), the NATO contract is awarded by a contracting agency or prime contractor of the NATO nation responsible for the infrastructure project.

10-704. NATO Facility Security Clearance Certificate. A NATO Facility Security Clearance Certificate (FSCC) is required for a contractor to negotiate or perform on a NATO classified contract A U.S. facility qualifies for a NATO FSCC if it has an equivalent U.S. FCL and its personnel have been briefed on NATO procedures. The CSA shall provide the NATO FSCC to the requesting activity. A NATO FSCC is not required for GCA contracts involving access to NATO classified information.

10-705. PCL Requirements. Access to NATO classified information requires a final PCL at the equivalent level.

10-706. NATO Briefings. Before having access to NATO classified information, employees shall be given a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO classified information. The FSO shall be initially briefed by a representative of the CSA if required by the contract. Annual refresher briefings shall also be conducted. When access to NATO classified information is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information. Certificates shall be maintained for 2 years for NATO SECRET and CONFIDENTIAL, and 3 years for COSMIC TOP SECRET and all ATOMAL information.The

contractor shall maintain a record of all NATO briefings and debriefings in the CSA-designated database.

10-708. Subcontracting for NATO Contracts. The contractor shall obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued prior to awarding the subcontract. The request for approval will be forwarded through the CSA.

10-710. Classification Guidance. Classification guidance shall be in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification. If adequate classification guidance is not received, the contractor shall contact the CSA for assistance. NATO classified documents and NATO information in other documents shall not be declassified or downgraded without the prior written consent of the originating activity. Recommendations concerning the declassification or downgrading of NATO classified information shall be forwarded to the CUSR.

CHAPTER 11
Miscellaneous Information

At this time, contracts at the 9Line facility do not have TEMPEST, DTIC, or IR&D requirements. If these requirements should change, the FSO will ensure that the NISPOM and other applicable government guidelines and procedures areimplemented.

9Line Additions to the SPP

9Line has worked on several classified contracts. While this does not mean that all information related to a particular contract is classified, it does highlight the need for sensitivity and caution by ALL 9Line EMPLOYEES (regardless of clearance) in dealing with the contractual subject matter. What follows is additional information to the 9Line Standard Practices and Procedures document to provide additional explanation of company procedures within the context of classified information, sensitive information and operational security. It is important to remember that this direction is not fully comprehensive; it would be impossible to anticipate the level of security and protocol detail required in every instance and we must always follow the policies and procedures of the client facilities where we are required to work. For that reason, 9Line employees should at all times endeavor to be wary of compromising surroundings and use common sense to protect our work!

Determining Authorization

Because the work that 9Line does is sensitive, there will be occasions where you will possess information (including materials) that other employees do not know. In these cases, it is incumbent upon you (the conveyor of the information) to determine whether the prospective recipient is authorized to receive that information. If the information at issue is classified, the conveyor will need to determine:

1) That the prospective recipient has been cleared (granted eligibility and access) at the level of the classified information in question (or at a higher level), and
2) That the prospective recipient has a need-to-know, that is, "a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program."

If the information at issue is not classified, but still sensitive, you need only determine the second criterion.

Clearance. You can quickly determine the clearance (eligibility and access level*)* of a prospective recipient by asking the 9Line's Facility Security Officer (FSO)/AFSO or the FSO of the facility where you are working. If in doubt, please ask the FSO or Assistant FSO (AFSO) first, *before* conveying the information.

Need-to-know. The "need-to-know" determination can be more difficult. 9Line encourages its employees to form the habit of asking, when appropriate: "Why do you need to know this information?" You must be fully satisfied with the reason given or refuse to divulge the information.

Simply put, "When in doubt, find out" by questioning your immediate supervisor. It is far better to delay disclosure to an authorized person than to disclose information to an unauthorized person.

9Line employees operate at all times on a "need to know" basis. This is as much for the company and clients' protection as it is for the employee.

Whether a 9Line employee needs to know information depends on whether that information is necessary to perform job functions – "Do I need to know this to do my job?" is a question the employee should ask himself/herself before exposure to and solicitation of information. In most cases, it should be clear to the employee based on the information available (i.e. the author/sender, the title of the document, or the other participants in the conversation) whether he/she will have a need to know.

Understandably, it may be difficult at times to make this determination without viewing the information beforehand. In these scenarios, the employee SHOULD NOT view the information without consulting the PM, COR, FSO, or AFSO first. That individual will make the determination.

There will also be times when an employee needs to know some, but not all information, within a given context. For example, an employee could need to know only some of the information contained in an email. Another example may be a conference call on which one of several agenda items pertain to an employee's work. As a policy, employees must seek to mitigate risk of exposure to unnecessary information by utilizing redacted versions of written documents (including emails) and politely removing themselves from conversations (including conference calls and VTCs) at appropriate times.

Notification

After the appropriate determinations have been correctly made, your obligation is not over. You must now advise the recipient of the classification of the information: Confidential, Secret or Top Secret

Legal Consequences

Unauthorized disclosure of classified information violates US Government regulations and contractual obligations and is punishable under federal law. If you are a cleared employee, when you gain knowledge of classified information, you become a legal custodian of that information. As such, your obligations are strict and are spelled out in the Classified Information Nondisclosure Agreement (SF 312) that you signed: "Intending to be legally bound, I hereby accept the obligations contained in this agreement in consideration of my being granted access to classified information," etc.

Changes to Personnel Status

Employees hired by 9Line will have eligibility (to view classified information), SECRET eligibility, TOP SECRET eligibility or SCI eligibility. The eligibilities are granted for a specific period of time. SECRET eligibilities are good for 10 years, while a TOP SECRET/SCI eligibility is good for five. These eligibilities are based on the information provided at the time the eligibility was granted. However, over time an employee's status may change and that could affect the eligibility held.

For example, a single employee who holds a TOP SECRET eligibility and then marries must notify the FSO to determine if the spouse will have an effect on the individual's eligibility status. Marriage to a foreign-born individual may have an adverse impact on an individual's clearance processing. While this in itself is not a reflection on the employee, Federal

regulations require the notification of a continuing relationship with a foreign national. This is especially critical if the individual holds a TOP SECRET clearance.

Drug use and/or conviction by local, state, or federal authorities may also affect an individual's clearance, depending on the severity of the charge. Once Security is notified of the event, a decision will be made as to whether the case must be referred to DSS or whether it can be handed internally. That decision will be made by the 9Line CEO/FSO.

Other areas of concern for the individual holding a clearance or attempting to obtain one may be that of a separation, a divorce, and/or garnishment of wages. Any one of these situations may have a negative impact on the individual's status, depending on whether a clearance action is currently being conducted to update a clearance or the individual is being processed for a new clearance. In effect, these situations may cause the investigative process to be slowed considerably and may require substantial time for a decision to be made by the investigating authority.

OPSEC

It only takes a relatively small amount of information leaked into the wrong hands to derail our current contracts and/or business development efforts. The "wrong hands" includes: activists, competitors, press and media, USG officials that are not the client.

In our line of work, operational security is very important to our current and potential clients. 9Line recognition as an "OpSec" leader will lead to greater client trust, which will in turn lead to more opportunity and more contracts.

Conversation. Perhaps the most difficult task in maintaining operational security is monitoring what we say to our friends, family and acquaintances. As a general guideline, it is permissible to say that 9Line is a government contractor, but we must be very cautious about discussing who our clients are, what products we deliver, or where we work. Although the people that we talk to everyday probably have no detrimental intention, they may still unknowingly reveal sensitive information (that a 9Line employee has provided them!) to someone who DOES have intentions to act in 9Line's or our client's detriment. Please also remember that while a particular detail of information may seem benign, that detail in conjunction with other information may be enough to result in a breach of operational security. So, when conversing with non-9Line employees, keep in mind that they may already know something about your company.

Computers/Emails. Critical files (including travel schedules, meeting itineraries, program information or personally identifiable information) must be encrypted when attached to an

email. In addition, any email that has sensitive information within the text must also be encrypted. Do not use a wireless connection to work on sensitive information unless you are on a password safe connection and set your Wireless to 'off' when not in use. When a computer is being replaced, clean and wipe the disks. Then remove the disks before disposing of the computer – destroy the disk via disassembly or shredder/crusher. If you have any questions on the use of computers/emails, please contact the FSO.

Every computer/laptop should be password protected; the password should be memorized, not written. Never check your laptop in your luggage and never leave your screen on without locking it.

Phone Calls. Avoid conversations on your cell phone in public. Also avoid customer related business calls on mobile phones anywhere. (Cell phones can and are being intercepted.) Never use hotel phones for business. Never use VoIP/Skype for sensitive business calls.

Written Documents. At the end of each workday, take a quick visual inventory to see if any sensitive documents have been left out. These documents should be stored in a desk drawer or filing cabinet. Shred all documents before putting them in the trash.

Press and Media. The CEO is the only 9Line employee that has authority to talk to the press. All other employees are required to take a message without confirming or denying anything.

Reporting Breaches: the actual, possible, the suspected and the attempted

In most instances, if 9Line employees follow the above guidelines and use common sense, there will be no security breaches. However, human nature is prone to error. For that reason, employees must report to the FSO or AFSO any actual breach, possible breach, suspected breach and attempted breach.

Upon any report of OpSec violation and at the discretion of the company CEO/FSO or AFSO, an investigation by the AFSO will commence. The AFSO will document a summary of the violation and the ensuing remedies, if any. Except in the most extreme circumstances where government mandates or applicable law requires it, all reports will be kept anonymous.

Counterintelligence. All employees and cleared consultants of 9Line must work hard to identify unlawful penetrators of 9Line and any other cleared U.S. defense industry organization and help articulate the threat for each other, industry and U.S. government leaders.

Report suspicious activities, behaviors, and contacts to your FSO as soon as possible.

Additionally, 9Line employees will be aware of the following **key CI focus areas**: Insider Threats, How to Report a Threat, Cyber Security, CI Integration, Elicitation, Foreign Travel Vulnerability, and Preparing for Foreign Visitors. Training on these focus areas will be required annually.

Violation of Policy

It is 9Line's policy to encourage honesty and transparency within the company when it comes to security. Therefore, there is a graduated scale of discipline for policy violations. Employees who violate the security procedures are subject to disciplinary actions by the 9Line leadership as follows:

- **First** violation (without compromise) within a period of 12 consecutive months—verbal reprimand.
- **Second** violation (without compromise) within a period of 12 consecutive months—written reprimand and report in JPAS.
- **Third** violation (without compromise) within a period of12 consecutive months—written reprimand and possible termination of employment.

- **First** violation (compromise) – written reprimand and report inJPAS.
- **Second** violation (compromise) - termination of employment if secondoccurs within twelve months of first violation.

Please also note that, depending on the gravity of the situation, there may be consequences and repercussions outside of 9Line's control. For example, a third party may take legal action against a 9Line employee individually. In such cases it is the policy of 9Line to NOT indemnify the individual. A violation of company operational security by an employee may also result in difficulty in obtaining or maintaining a US security clearance.

Security Briefings

All cleared employees are required to have a security briefing prior to being given access to classified material. Aside from the education contained in this document, the briefing will include:

- A Threat Awareness and Defense Security Briefing
- An Employee Reporting Obligation Briefing
- A Security Classification Briefing

- Foreign Travel – Employees must report it prior to travel and then complete a briefing on threats to the specific location and back-brief anything significant upon return from the trip overseas.
- Insider Threat

At least annually, 9Line will conduct refresher briefings of all cleared employees. The purpose is:

- To remind cleared employees of their continuing responsibilities for safeguarding classified information.
- To ensure that cleared employees are aware of the security procedures pertaining to their particular work assignment.
- To ensure that cleared employees are aware of any security deficiencies uncovered during inspections that required their individual attention to correct.
- To educate employees in the methods and operations employed by hostile intelligence organizations.
- To detail defensive measures to counter such subversion attempts.

Refresher briefings are intended to reinforce the information provided during the initial briefing and to inform employees of relevant changes in the NISPOM and SPP. They will be distributed to all employees during the first quarter of each calendar year. Additionally, all 9Line employees will receive a security de-briefing prior to departure from the company for any reason.

I,_____am a cleared/uncleared employee/contractor of 9Line. I have read the 9Line Standard Practices and Procedures Manual/Policy regarding the company's security and operational procedures and am aware of my responsibilities therein. In addition, I have been briefed on the following as applicable:

- My eligibility and access level (SCI/Top Secret / Secret/Confidential)
- The length of time and location of myemploy
- Guidance that I am only authorized access to classified information at that location and to not transport information without the approval of the FSO
- Direction that I am required to comply with the security requirements and procedures at the host facility where I am viewing classifiedinformation
- Warnings not to discuss classified information outside of the work site or over a non-secure phone
- Any procedures for the safeguarding of classified information that are specifically associated with my job.

Signed:_____

Date:_____