

Operations Security (OPSEC) Plan

[Company / Organization]

[Company CAGE CODE]

Contract/Solicitation: [#####-##-#-####]

Prepared by: [Company/Organization FSO or Security Representative]

[OPSEC Plan approval date]

[Include / List distribution controls and/or handling caveats if applicable]

I. INTRODUCTION.

A. Purpose. The purpose of this OPSEC Plan is to establish and document the proper procedures and define the responsibilities for implementation of the overall OPSEC requirements associate with Contract/Solicitation: [#####-##-#-#####]. This OPSEC plan will provide instruction to all employees ensure protection and safeguarding of [supported GCA] critical information. This plan sets forth procedures for protecting [Company] Facility and Government Contracting Activity (GCA) critical, propriety and sensitive information and data. The OPSEC Plan outlines the OPSEC Process utilized to identify critical information, assess threats, assess and identify vulnerabilities, analyze the associated risks; and to apply appropriate and cost effective countermeasures to mitigate or eliminate potential or actual identified threats. This plan will provide information designed to show [Company] personnel what information needs to be protected, what the threat is, what the potential vulnerabilities are, what to do with the risk, and what countermeasures can be applied to prevent information loss.

B. Scope. This plan was established to provide a comprehensive OPSEC focus with regard to OPSEC policy guidance and procedures required by the National Industrial Security Operating Manual (NISPOM) and [Company], and other DoD regulatory requirements as they pertain to cleared industry. Changes to this OPSEC Plan will be coordinated with the [Company] Facility stakeholders and the [Company] Facility Security officer. This OPSEC Plan is applicable to [Company / Location /CAGE Code] off-sites and any sub-contractors. For any work conducted at Customer locations, that facility's OPSEC Plan applies. If any conflict regarding the Contract, the NISPOM or [Company's] security requirements or procedures arises, the Facility Security Officer or designated Program Security Representative will coordinate with the GCA Security Point of Contact and any other applicable Government Agency (i.e., the Defense Counterintelligence and Security Agency-DCSA) for a resolution.

C. Applicability. This OPSEC Plan applies to all solicitations and awarded contracts by consultants, and sub-contractors under this contract, sub contract, project and task when imposed by the DD Form 254. All applicable [Company] personnel will review this document and become familiar with not only the guidance detailed in this plan but also the OPSEC process employed to develop these concepts. Adherence to this OPSEC Plan will be the responsibility of the [Company] Facility Security Officer (FSO) and associated Program Manager(s). The OPSEC plan will also apply to the activities of any sub-contractor and international sub-contractors receive OPSEC guidance with an approved DD Form 254, as applicable.

D. Security Responsibilities.

1. [Company] Facility Security Officer/Program Security Representative is the direct interface with the customer regarding OPSEC matters. They have the following responsibilities:

- Execute the OPSEC instructions and give guidance when questions arise by [Company] employees.
- Author changes and revisions to this document will be reviewed by the supported GCA prior to implementation.
- Assist program teams in executing the OPSEC requirements and procedures stated in the contract, those of [Company] and the NISPOM.

- Monitoring the implementation and day-to-day management of OPSEC policies and procedures.
- Facilitate open dialogue and to share knowledge between the program management team, security functions at all participating program locations and the customer, when needed.

2. Additionally, it is the responsibility of all [Company] security personnel working under referenced contract to adhere to OPSEC planning requirements outlined in this document and as delineated directly by [Company] security personnel. All personnel are responsible for the successful implementation of this plan. [Company] will be responsible for OPSEC training of personnel working under this contract. All personnel supporting the contract will receive initial OPSEC awareness training and annual OPSEC refresher training. The FSO or company Security Representative will coordinate the implementation of training, administration, and execution of this plan with the GCA. The FSO or [Company] Security Representative will maintain records of OPSEC training completion by applicable personnel and also ensure that all procedures identified in this Plan are followed. The GCA security office will support the FSO or [Company] Security Representative in the development, implementation, and compliance with the procedures established in this OPSEC Plan.

II. OPSEC PROCESS. OPSEC is a systematic and proven process [Company] employees can implement to deny potential adversaries information about [supported GCA] associated capabilities, activities, limitations and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The OPSEC process is most effective when fully integrated into all planning and operational processes. The OPSEC process involves five steps:

- Identification of Critical Information (CI) and Indicators
- Threat characterization
- Analysis of vulnerabilities
- Assessment of risk
- Application of appropriate countermeasures

A. Critical Information (CI).

1. CI is generally unclassified information and specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment. Although some critical information is classified when pertaining to national security issues such as military or intelligence operations, other unclassified information is not afforded the same protection. It is this unclassified information, or indicators thereof, which, when considered in aggregate, may provide an adversary with clues to other more critical data. The process to identify CI usually begins with an examination of the totality of a project or operation to determine what exploitable but unclassified evidence of sensitive or classified activity is vulnerable to adversary collection and exploitation. Such evidence is usually derived from openly available data or observable activities. Certain 'indicators' may be pieced together or correctly interpreted to discern or ascertain critical information or accurate conclusions. Indicators commonly stem from the routine administrative, physical, or technical actions or activities taken to prepare for or execute a project or operation.

2. CI is valuable to an adversary, and if obtained, this information will either impact the success of the work being performed pursuant to the contact, to include operations, activities, and mission; or improve the likelihood of an adversary meeting their goals. The supported GCA's Critical Information List includes but is not limited to information such as the following: [Company] FSO can also include specific company sensitive/critical/proprietary information.]

- Operations, missions, and exercises;
- Test schedule or specific test location;
- Off-base movement of classified or sensitive information or arms, ammunition, and explosives (AA&E);
- Location of sensitive equipment (AA&E, COMSEC, etc.) or sensitive facilities (e.g., restricted areas or laboratories);
- Force structure and readiness, such as recall rosters;
- Capabilities, vulnerabilities, and limitations;
- Security weaknesses;
- Existence and/or details of intrusions into or attacks against [Company] Security networks or information systems;
- Network (and system) user IDs and passwords;
- Movements of key command personnel or visiting dignitaries, including itineraries, meeting agendas, hotel and transportation reservations, plans/routes, etc.; and
- Security classification of equipment, systems, operations, etc.

B. Indicators. Data derived from friendly detectable actions and open-source information adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. Indicators may be classified or unclassified. Indicators are data derived from open (unprotected) sources or detectable actions. These indicators may be prevalent in [Company] daily routines, such as administrative, operational and logistical activities. Indicators are activities that can be heard, observed, or imagined, which could compromise mission critical information. Indicators obtained by an adversary or competitor could result in knowledge or actions harmful to friendly intentions. Indicators include such things as personnel or material actions and movements that can be observed, including public releases, conversations or documents, and habitual procedures when conducting a given type of operation or test. All detectable indicators that convey or infer critical information must be identified and protected if determined vulnerable. Example of potential indicators (list not all inclusive):

- Changes to test site configurations, logistical enhancements.
- Increased presence of gov't affiliated personnel at test and evaluation sites.
- Thermal signature of associated facilities/buildings.
- Presence or absence of vehicles and support equipment.
- Temporary construction.
- Manpower increase of on-site personnel.
- Additional security personnel/guards.
- 24-hour ops or alternate work hours (from a routine schedule).
- Units/organizations not based at or assigned to the facility.

- Dress, appearance, uniforms, badges of visitors signifying sponsorships or affiliations with certain commercial companies or DoD agencies.
- Increase in presence of emergency personnel/equipment.
- Embarking or moving special equipment.
- Prepositioning equipment or supplies.
- Detection of increased radio/signal traffic.
- News/Press releases.
- Public notice of outside activities.

C. Threat. Knowing who the adversaries are and what information they require to meet their objectives is essential in determining what information is truly critical. In any given situation, there is likely to be more than one adversary and each may be interested in different types of information. Analyzing the threat is a necessary step in evaluating and developing appropriate countermeasures. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators. Today, foreign intelligence services, criminals, and private sector industrial espionage threats are focused on American industry and the private sector. Their efforts compromise intellectual property, trade secrets, and technological developments that are critical to national security. Espionage against the private sector increases the danger to long-term U.S. prosperity. Counterintelligence is a challenge for corporations for two reasons. Cost is the first reason. Counterintelligence measures absorb company resources that would otherwise be used for growth. The second counterintelligence challenge is tied to the nature of public corporations. American companies are driven into developing markets by shareholders, growth ambitions, and the desire to beat Wall Street's quarterly earnings expectations. The requirement to move quickly and unabashedly can leave American companies vulnerable as they flock into potentially spy-rich developing nations. It can be presumed the threat to [Company] contract support activities is ongoing. Although there may be no eminent identified threat, exploited critical information can negatively impact success. [Company] may be subject to collection efforts by adversaries, who employ both overt and covert methods. The adversaries' ability to collect information using the full range of intelligence disciplines must be considered. Below are examples of threats and collection methods utilized to gather critical and sensitive information (not all inclusive):

1. Human Intelligence (HUMINT) Threat. HUMINT is the collection of information through the use of human sources. It is gathered either covertly by espionage agents with placement and access or overtly through information available in the public domain. A high priority is assigned to the acquisition of scientific and technical information concerning the research and development of [Company] military technology and industrial techniques and processes, and related military and strategic capabilities. This information is collected primarily to anticipate military application of technological breakthroughs and to foster scientific, mechanical, and industrial support of the collector's strategic force. HUMINT threats can include:

a. Espionage Agents – Intelligence agents are assigned and tasked to target DoD contractor personnel, particularly research, development, test and evaluation (RDT&E) efforts. The individual intelligence agents will use people in an attempt to develop any information they can use.

b. Foreign Visitors – The presence of foreign visitors, either in an official status or as the casual tourist, increase the risk of intelligence collection efforts.

c. Insider Threats – [Company] employees with access who have the opportunity, capability, and intent to purposefully compromise sensitive information and/or materials for distribution to entities who pose a risk to [Company] and U.S. security interests. [Company] employees must maintain vigilance of their coworkers for potential insider threats; report their concerns and continuously implement safeguards for protecting [Company] capabilities. This includes improved counterintelligence analysis of audit and access controls, and improving [Company] ability to detect and respond to insider threats.

2. Open Source Intelligence (OSINT) Threat. Foreign intelligence collection services satisfy the majority of their intelligence collection requirements through the systematic analysis of open sources (e.g., publicly accessible). Such information may be obtained through the news media, official and unofficial organization and professional publications, the World Wide Web (WWW)/internet, the National Technical Information Center (NTIC), the Defense Technical Information Center (DTIC), at symposiums and seminars, university/college affiliations, or through contractor advertisements. To put the OSINT threat into the proper context, consider that the total number of dedicated foreign agents in this country is estimated to be between one and two thousand, while the total number of reporters in this country is closer to one million; a thousand to one ratio. U.S. adversaries depend heavily on OSINT to assist them and are much more likely to learn of our critical information through open sources. It has been estimated 90% of the information needed by adversaries is available through open sources.

3. Signals Intelligence (SIGINT) Threat. This collection method includes communications intelligence (COMINT), electronic intelligence (ELINT), and telemetry intelligence (TELINT) or measurement and signature intelligence (MASINT). This threat targets telephones (including cellular, pagers, and residential), radio transmissions, and facsimile transmissions. Exploitation is much easier when any deviation from standard security practices occurs. The most common error is discussion of critical information over unsecured telecommunications means (i.e., non-secure telephone, facsimile or email). Intelligence personnel with mobile collection equipment sometimes perform signals collection efforts within close proximity to government and contractor facilities and test ranges. Foreign SIGINT capabilities that pose a threat include:

- Fixed ground collection stations, including several embassies and embassy-related facilities
- Space-borne SIGINT platforms capable of intercept of radio frequency emitters
- Ocean-going vessels specifically designed for intelligence gathering known as Auxiliary General Intelligence (AGI)
- Merchant ships
- Intercept of telephone relay microwave links

4. Imagery Intelligence (IMINT) Threat. IMINT describes the capability to derive information from imagery developed over the full range of the electromagnetic spectrum. IMINT frequently provides very valuable intelligence. It can be collected via the use of cameras and imaging devices mounted in airplanes, ships, space vehicles, ground vehicles, or carried by individuals on land. IMINT can provide the adversary with an extremely valuable collection and

analysis tool, especially during the testing and evaluation stages of systems development. The most serious threat from IMINT resources at the national level stems from photoreconnaissance satellites. IMINT threats against the U.S. can include, but are not limited to:

- Satellites
- Manned space stations
- Commercial and private aircraft overflights
- Ground vehicles (commercial, private and government affiliated)
- Drones/Unmanned Aerial Vehicles
- Unauthorized use of copying/duplicating equipment
- Military/government aircraft (e.g., Treaty on Open Skies platforms)
- Maritime/seaborne platforms (commercial, private and government affiliated)
- Personnel electronic devices (i.e., cell/smart phones, still/video cameras, etc.)

5. [Company] security personnel must also consider an adversary threat's ability to process and analyze that information, as well as their intention and capability to pose a credible threat. If any element of this threat analysis is missing, the threat is eliminated. For example, a group that desires information contained in encrypted radio transmissions, but does not have the capability to obtain it, is not a threat, while a group that desires to know when a cutter or aircraft departs its unit, and can observe it, is surely a threat. The objective, therefore, of threat analysis is to know as much as possible about each adversary and the strategies/options available to them for targeting the unit and its operations. It is also important to analyze the adversarial threat within the context of an actual operation, mission, project, etc., and, to the extent possible, determine what the adversaries' capabilities will be for the specific time and location of [Company] programs, projects and capabilities.

D. Vulnerability Analysis. Determining vulnerabilities involves conducting a detailed analysis of how an operation is normally conducted. The operation must be viewed from the adversarial perspective. An OPSEC vulnerability exists when the adversary is capable of collecting critical information or indicators, analyzing them, and then acting quickly enough to impact [Company] objectives. Determine what an adversary needs to know and where the information is available, it is necessary to determine if it is possible that the adversary could acquire and exploit the information to diminish or preclude our success. What are the vulnerabilities (weaknesses) and indicators (clues) which an adversary could exploit to direct their collection efforts? Vulnerabilities would also include an adversary's ability to acquire instrumentation design information; data processing support files or other data processing information, which would be useful in interpreting test data; test data; test reports, including briefings, summaries, interim reports, technical papers/publications, and final reports. Analysis of vulnerabilities helps identify OPSEC countermeasures required to protect sensitive information under [Company's] control. The most desirable OPSEC countermeasures combine the highest protection with the least impact on the [Company's] effectiveness.

1. Examples of vulnerabilities and indicators which an adversary could exploit can include (but are not limited to):

- Discussion of program specifics with individuals without a need-to know.
- Discussion of sensitive project information on an unsecure telephone or via unencrypted emails.

- An adversary's ability to observe and monitor activities and personnel involved in specific projects.
- Sharing of project related information and activities in social media forums.
- Research and other sensitive information available in the public domain (e.g., publications, internet, waste materials (i.e., dumpster diving)).
- Elicitation of research and other project information at international conferences, meetings, and social settings
- Outdoor testing which results in exposure of program/activities to observation
- Sympathies of personnel for adversary countries (disgruntled employees, insider threats).

2. Vulnerabilities and Associated Threats (list not all inclusive):

a. HUMINT:

- Discussing sensitive information in areas where it can be overheard by unauthorized persons.
- Failing to report individuals or actions that are damaging to security.
- Disgruntled employees with authorized access (e.g., insider threats).
- Lack of proper escorting responsibilities (RE: foreign visitors).
- Lack of knowledge of foreign threats and collection capabilities.
- Personnel susceptibility to elicitation or espionage (insider).
- Lack of security awareness signage and warning notices prominently displayed in program/project work areas.

b. SIGINT:

- Unencrypted voice communications equipment and devices.
- Telecommunications transmitted via microwave links.
- Unapproved and unaccredited IT and ADP equipment used to process sensitive/classified data.
- TEMPEST and compromising emanations.
- Neglecting to utilize encryption devices for conducting routine classified communications (as applicable).
- Voice telecommunications devices modified to serve as clandestine listening devices.
- Unauthorized telecommunication devices in areas where classified and sensitive information is routinely discussed.
- Unfamiliar with locations of secure telecommunications equipment.
- Integrated commercial telecommunications infrastructure (i.e., public switched networks).

c. OSINT:

- Discussing sensitive information on social network sites/personal blogs.
- Posting sensitive information in the internet.
- Using personal e-mail to communicate official business.

- Sensitive, official information revealed in public media (e.g. brochures and magazines).
- Discussion of sensitive activities/operations in public setting.

d. IMINT:

- Failure to implement cover, concealment and deceptions actions.
- Outdoor testing of sensitive systems, platforms and activities.
- Ground vehicles parked near fence lines of facilities and installations.
- Personnel electronic devices (i.e., cell phones, smart phones, still cameras, iPads, video, etc.) with photographic capabilities.

E. Risk Assessment. Risk assessment is the process of evaluating the risks to critical information based on susceptibility to intelligence collection and the anticipated severity of loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity. It involves assessing the adversary's ability to exploit vulnerabilities, which would lead to the exposure of critical information and the potential impact it would have on [Company] activities and operations. Risk assessment is essentially the process of balancing vulnerability against the threat, then deciding if the residual risk warrants application of countermeasures. Included in the assessment of an adversary's capability is not only their ability to collect the information but also their capability to process and exploit (evaluate, analyze, interpret) the vulnerability in time to make use of the information. In mathematical terms, a risk formula looks like this:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

In order to assess risk to an asset (e.g., information, property and/or people) three conditions must be present: (1) one or more vulnerabilities, (2) a threat, and (3) an impact or consequence. The absence of a threat or vulnerability removes the risk. The absence of an identified consequence does not in every case eliminate risk but certainly does mitigate it, (i.e. make it more acceptable). Vulnerabilities and threats must be correlated. Where [Company's] vulnerabilities are exploitable and adversary threat capabilities and intentions are present, the risk of adversarial exploitation must be anticipated. Therefore, a higher priority for protection needs to be assigned and countermeasures applied. Conversely, where the vulnerability is moderate or slight and the adversary has a limited collection capability, the priority may be medium to low. List of steps to help determine potential or actual risks (not all inclusive):

- What is the likely impact of an OPSEC measure on operational effectiveness if implemented?
- What is the probable risk to mission success if [Company] does not implement an OPSEC measure?
- What is the probable risk to mission success if an OPSEC measure does not work?
- What is the impact on future missions if a specific measure is adopted and successful?

F. Countermeasures. A countermeasure is anything (e.g., action, process, procedure, etc.) that effectively negates an adversary's ability to exploit vulnerabilities. Appropriate cost-effective countermeasures to minimize or mitigate vulnerabilities, threats, and the utility of critical

information to adversaries must be developed. These countermeasures must be designed to defeat or delay adversarial actions to a point of acceptable risk. Countermeasures may include procedural changes, suppression of indicators to deny critical information, deception, perception management, intelligence countermeasures, traditional security measures, or any other action that is likely to work in a given situation. There are no standard solutions for all circumstances. This process requires continual evaluation and creativity. Periodic evaluation of countermeasures by [Company] Security Reps is necessary to assess their continual effectiveness, but also to determine if the countermeasures themselves have become an indicator. Perhaps the most cost-effective measure a unit can take is to adopt an active training and awareness program. Countermeasure development and application should be designed to prevent an adversary from detecting critical information; provide an alternative interpretation of critical information or indicators; or deny the adversary's collection system. All [Company] critical information, to include [supported GCA] critical information accessed in support of referenced contractor support activities must be protected. Examples of countermeasures (list not all inclusive):

- Encrypted and digitally signed emails
- Safeguard critical information as CUI
- Using secure telecommunication (secure phones and facsimiles)
- Utilize secure transmissions capabilities (such as AMRDEC SAFE)
- Practicing need-to-know when sharing sensitive information
- Proper disposal of printed material (i.e., shredding or burning)
- Do not discard printed material in recycle bins or trash receptacles
- Secure containers and rooms where sensitive information resides
- Implement effective security education, training and awareness (SETA)
- Brief program personnel on unique/special security requirements
- Integrate OPSEC with other core security disciplines as applicable
- Don't share specified passwords/log-on procedures with others
- Ensure personnel are familiar with security policies and guidelines
- Conduct random security spot checks of work centers for compliance
- Properly identify/mark sensitive information to ensure proper handling
- Properly identify/mark IT systems and media
- Implement an effect public release review process
- Employ camouflage, cover, and concealment techniques (i.e., tarps, covers, hangars, etc.) to hide sensitive equipment/systems
- Security review of official or proprietary information before public release
- Robust visitor control and escort procedures
- Flow-down of OPSEC requirements and procedures to sub-contractors

III. RESOURCES.

A. The primary source of counterintelligence support for the US Navy is the Naval Criminal Investigative Service (NCIS) (<https://www.ncis.navy.mil/>). NCIS serves as the coordinating authority of all DON counterintelligence activities and is the lead agency for the conduct of offensive counterintelligence operations, which seek to penetrate and neutralize adversary intelligence services. NCIS works to neutralize foreign intelligence services and foreign commercial activities seeking information about critical naval programs and research, development, test and evaluation facilities. The NCIS Multiple Threat Alert Center is responsible for collecting, analyzing, and disseminating information regarding criminal, terrorist, foreign

intelligence, cyber, and other threats. It also has responsibility for providing worldwide asymmetric threat warning to DON through the operation of a 24/7 watch center dedicated to this task. The [Company] FSO, via the supported GCA security element, can solicit local NCIS support for threat awareness assistance such as threat briefings.

B. The National Counterintelligence and Security Center (NCSC) leads and supports the counterintelligence and security activities of the US Government, the US Intelligence Community, and US private sector entities who are at risk of intelligence collection, penetration or attack by foreign and other adversaries. As stated earlier, foreign intelligence services, criminals, and private sector spies are focused on American industry and the private sector. These adversaries use traditional intelligence tradecraft against vulnerable American companies, and they increasingly view the cyber environment—where nearly all important business and technology information now resides—as a fast, efficient, and safe way to penetrate the foundations of our economy. Espionage against the private sector increases the danger to long-term U.S. prosperity. Additional counterintelligence and threat assessment information can be found at <https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-threat-assessments-mission/ncsc-economic-espionage>.

C. The Defense Counterintelligence and Security Agency (DCSA) oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program by providing professional risk management services. DCSA's counterintelligence element identifies threats to U.S. technology and programs resident in cleared industry, and articulates that threat to stakeholders.

1. The DCSA premier unclassified publication for counterintelligence, *'Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting'*, analyzes possible foreign targeting of information and technologies developed or maintained within the cleared contractor community. The principal substance of this report is drawn from DCSA analysis of suspicious contact reports received from industry. It offers a single perspective of the threat, as illustrated by industry's unsolicited contact with foreign entities interested in defense programs and products. This publication identifies foreign collection trends directed at U.S. defense industry so that U.S. technologies may be better protected. This document identifies the most frequently targeted U.S. technologies, the preferred collection methods, entities attempting the collection, and the regions where collection originates. This publication is available via the DCSA webpage hosted on 'intellipedia.intelink.gov' and also on the Department of Homeland Security Information Network, both are restricted access websites.

2. DCSA also offers a companion product to their annual 'Targeting U.S. Technologies' report, which is an information sheet identifying the seven most commonly targeted technology categories. This information sheet and other counterintelligence reference products can be access via the DCSA public website at <https://www.dss.mil/ma/ctp/ci/>.

3. Another part of the DCSA mission, in support of the National Industrial Security Program, is the accomplishment of 'vulnerability assessments' of all cleared contractor facilities under its cognizance. The focus of vulnerability assessments is to ensure facilities are compliant with NISPOM requirements to ensure safeguards employed by contractors are adequate for the protection of classified information. Following each assessment DCSA will provide the cleared company FSO a list of identified vulnerabilities and recommended actions to remedy. The DCSA

Vulnerability Ratings Matrix product can be accessed via their official web site at:
https://www.dss.mil/Portals/69/documents/io/tools/VulnAssm_RatingMatrix_2016Update.pdf.

D. [Company] personnel with appropriate security clearance and access to classified networks such as SIPRNET, can also access current classified threat products and provide up-to-date briefings of potential or actual adversary threats targeting contractor support activities. Validate security clearance of audience members prior to presenting classified briefings.

E. Applicable OPSEC References:

- The National Industrial Security Operating Manual (NISPOM) dated February 2006 incorporating Change 1, of March 23, 2018, and subsequent revisions.
- DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual, of 3 Nov 2008, incorporating Change 1, 26 Apr 2018 and subsequent revisions
- SECNAVINST 3070.2A, Operations Security, of 9 May 19
- [Supported GCA] Critical Information List
- Other documents as contractually required (i.e., DD254).

IV. LISTING OF APPLICABLE POINTS OF CONTACT.

- [Company FSO],
- DCSA,
- Supported GCA (PM, KOR, Security),
- NCIS,
- Etc.