CUI/OPSEC GUIDANCE

1.1 INFORMATION SECURITY

The contractor will be provided ***Federal contract information***[1]or ***Controlled defense information***[2] which includes but is not limited to ***Controlled unclassified information (CUI)***[3], ***Controlled technical information***[4], ***Contractor attributional/proprietary information***[5], *etc.* (hereinafter collectively called "*CUI*") under this solicitation, contract, task order, or delivery order (hereinafter collectively referred to as "*acquisition*").

According to FAR 52.204-21, DFARS 252.204-7012 and DoDI 5200.48 "Controlled Unclassified Information" (CUI) (06 March 2020) the contractor shall provide ***adequate security***[6] for all *CUI* residing on or passing through non-DoD information systems including all subcontractor information systems utilized in support of the *acquisition*. The contractor shall only disseminate *CUI* within the scope of assigned duties and with a clear expectation that confidentiality is preserved. In accordance with (IAW) SECNAVINST 5510.36B, DON Information Security Program (Jul 16, 2019) all Department of the Navy (DON) employees including contractors shall be personally and individually responsible for properly protecting classified information and *CUI* under their custody and control and shall ensure classified information and *CUI* are protected IAW the same and Volumes 1 thru 3 of DoDM 5200.01, DoD Information Security Program of 24 Feb 2012 (Incorporating Change 1, Effective May 9, 2018) and DoDI 5200.48.

1.1.2 Information Safeguarding Requirements

The contractor shall protect/safeguard *CUI* and shall provide compliance documentation validating they are meeting this requirement in accordance with DFARS 252.204-7012. Certain information provided by the government under this *acquisition*, requires unique handling, storage, marking, and/or release/dissemination procedures (see Addendum "A" CONTRACTOR OPSEC GUIDANCE" for specific details which is/are incorporated in full by reference herein). Contractor is cautioned to study Addendum "A" and comply accordingly.

[1] In accordance with FAR 4.1901 ***"Federal contract information"*** means: information, not intended for public release, that is provide by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on a public Web site) or simple transactional information, such as that necessary to process payments.

[2] In accordance with DFARS 252.204-7012 ***"Covered defense information"*** means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at https://www.archives.gov/cui/registry/category-list, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

[3] In accordance with 32 CFR Part 2002 ***"Controlled Unclassified Information"*** means information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

[4] In accordance with DFARS 252.204-7012 ***"Controlled technical information"*** means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

[5] In accordance with DFARS 252.204-7012 **"Contractor attributional/proprietary information"** means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

[6] In accordance with DFARS 252.204-7012 **"Adequate security"** means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

The contractor shall track all "*CUI*" associated with its execution and performance under this *acquisition*. The contractor shall document, maintain, and provide the Government, a record of subcontractors, vendors, and/or suppliers who will receive or develop *CUI* who are associated with the execution and performance of this *acquisition*. Contractor shall restrict unnecessary sharing and/or flow down of *CUI* associated with execution and performance under this *acquisition*. Contractor shall restrict unnecessary sharing and/or flow down of *CUI* based on a 'need-to-know' to execute and perform the requirements under this *acquisition*. Contractor shall flow down the requirements specified in this section to its subcontractors, vendors, and/or suppliers.

All contractor and subcontractor personnel assigned to this *acquisition*, shall complete annually the Center for Development of Security Excellence (CDSE) "DoD CUI Mandatory Controlled Unclassified Information ("CUI) Training" located on the CDSE *eLearning* website at https://www.dodcui.mil, or similar Contracting Officer approved annual *CUI* training, no later than 30 September of each year. Contractors and their subcontractors will report to NAVFAC FE by 15 October each year the number of their employees assigned to the *acquisition*, who were trained, the number remaining to be trained, and the completion percentage. Failure to comply with the requirement for annual *CUI* training may result in termination of the *acquisition* and may be reported as non-compliant with NAVFAC *CUI* requirements. The point of contact (POC) for reporting annual *CUI* training under this *acquisition* is the Contracting Officer's Representative, or the Contracting Officer if the POC is unavailable.

1.1.3 Disclosure of Information Requirements

In accordance with DFARS Clause 252.204-7000, Disclosure of information, contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and/or Contractor personnel who have a "need to know." Contractor shall not use any information or documentation provided by the Government or developed under this *acquisition*, for other purposes without the consent of the Government Contracting Officer IAW DFARS 252.204-7000. Contractor shall not release to anyone outside the Contractor's organization any *CUI*, regardless of medium (e.g., film, tape, document, etc.), pertaining to any part of this *acquisition*, or any program related to the same, unless the Contracting Officer has given prior written approval IAW DFARS 252.204-7000. ***Markings***: All deliverables/submittals generated by the Contractor under this *acquisition* shall be properly marked in accordance with DoDI 5200.48. Technical information[7] and *CTI* shall also be marked with appropriate Distribution Statements and Export Control warnings in accordance with DoDD 5230.24, Distribution Statements on Technical Documents (Oct. 15, 2018) and program Security Classification Guidance.

1.1.4. Operations Security (OPSEC) Requirements

Information Security programs are usually oriented towards the protection of classified information and materials. Operations Security (OPSEC) involves the protection of critical information focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E, Department of Defense Operations Security (OPSEC) Program (May 11, 2018), SECNAVINST 3070.2A, OPERATIONS SECURITY (9 May 2019), SECNAVINST 5510.36B, DON INFORMATION SECURITY PROGRAM (Jul 16 2019), and NAVFACFEINST 3432.1 (24 AUG 2017), NAVFAC FE's OPSEC program implements requirements in DoD 5205.02, DoD Operations Security (OPSEC) Program Manual (November 3, 2008, Incorporating Change 1, Effective April 26, 2018). OPSEC requirements are applicable when contractor personnel have access to or generate *CUI* as defined in DFARS 225.204-7012. As such, OPSEC Measures (i.e., the planned action to conceal or protect identified critical information and indicators from disclosure, observation, or detection and to protect

[7] In accordance with DFARS 252.204-7012 **"Technical information"** means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013 , Rights in Technical Data—
Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

the same from collection) are applicable to this *acquisition*. Contractor is cautioned to study Addendum "A" and comply accordingly.

All contractor and subcontractor personnel shall comply with NAVFACFEINST 3432.1 (24 AUG 2017). NAVFACFEINST 3432.1 is available from the Contracting Office. All contractor and subcontractor personnel assigned to this *acquisition*, shall complete annually the Center for Development of Security Excellence (CDSE) "OPSEC Awareness for Military Members, DoD Employees and Contractors" located on the CDSE *eLearning* website at https://www.cdse.edu/toolkits/deliveruncompromised/index.html, or similar Contracting Officer approved annual OPSEC training, no later than 30 September of each year. Contractors and their subcontractors will report to NAVFAC FE by 15 October each year the number of their employees assigned to the *acquisition*, who were trained, the number remaining to be trained, and the completion percentage. Failure to comply with the requirement for annual OPSEC training may result in termination of the *acquisition* and may be reported as non-compliant with NAVFAC OPSEC requirements. The point of contact (POC) for reporting annual OPSEC training under this *acquisition* is Contracting Officer's Representative, or the Contracting Officer if the POC is unavailable.

Note: the following clauses have been incorporated in this *acquisition* - DFARS 252.204.7000 Disclosure of Information, 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls, 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, and 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. DFARS Clause 252.204-7000 restricts the release of unclassified information outside contractor's organization without prior Contracting Officer permission, with exceptions; DFARS Clause 252.204-7008 requires contractor compliance with Safeguarding Covered Defense Information Controls; DFARS Clause 252.204-7009 limits the use or disclosure of contractor reported cyber incident information, and DFARS 252.204-7012 requires contractor to provide adequate security for all covered contractor information systems (including implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" in effect at the acquisition is issued) and to comply with cyber incident reporting requirements.

1.1.5. Violations of the Information Security Requirement

A knowing, willful, or negligent failure to comply with the above-referenced Information Security requirements may result in criminal penalties under applicable Federal law, as well as administrative remedies including but not limited to termination of the *acquisition*.

ADDENDUM "A"
CONTRACTOR OPSEC GUIDANCE

1. Purpose. This document provides Operations Security (OPSEC)***** guidance to Offerors/Contractors (i.e., corporations and businesses, etc.) who are provided *Federal Contract Information (FCI)* and process or store the same on a *covered contractor information system)(FAR 52.204-21).* This OPSEC guidance also applies to *covered defense information* (CDI), *controlled technical information* (CTI) or other information (as described in the *controlled unclassified information* (CUI) Registry at https://www.archives.gov/cui/registry/category-list (DFARS 252.204-7012); and said information is referred to in a *solicitation, contract, task order, or delivery order* (hereinafter called "*acquisition*"). May also include *contractor attributional/proprietary information* (CPI), *personally identifiable information* (PII), *critical information* (CI) or *sensitive information* (SI)) that is inappropriate for release to the public and that requires *safeguarding* or *dissemination controls* pursuant to and consistent with law, regulations, and Government wide policies (DoDI 5200.48, Controlled Unclassified Information (CUI)(06 Mar 2020).

*****OPSEC involves the protection of critical information focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E, Department of Defense Operations Security (OPSEC) Program (May 11, 2018) and NAVFACFEINST 3432.1 (24 AUG 2017), NAVFAC FE's OPSEC program implements requirements in the DoD 5205.02-M - OPSEC Program Manual. OPSEC requirements are applicable when contractor personnel have access to or generate *CDI* as defined in DFARS 225.204-7012. As such, OPSEC Measures (i.e., the planned action to conceal or protect identified critical information and indicators from disclosure, observation, or detection and to protect the same from collection) are applicable to this requirement. Contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and/or Contractor personnel who have a "need to know." Contractor shall not use any information or documentation provided by the Government or developed under this *acquisition* for other purposes without the consent of the Government Contracting Officer IAW DFARS 252.204-7000. Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document, etc.), pertaining to any part of this *acquisition* or any program related to the same, unless the Contracting Officer has given prior written approval IAW DFARS 252.204-7000. ***Markings***: All deliverables/submittals generated by the Contractor shall be properly marked. For Official Use Only information generated and/or provided under this contract shall be marked in accordance with DoDI 5200.48. Technical information shall also be marked with appropriate Distribution Statements and Export Control warnings in accordance with DoDD 5230.24 and program Security Classification Guidance.

Certain information provided by the government may require unique handling, storage and or release/dissemination procedures. Contractors are cautioned to study the "CONTRACTOR DUTIES & RESPONSIBILITIES" provided herein and comply accordingly.

Note: the following provisions/clauses have been incorporated in this solicitation/contract – FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems, DFARS 252.204.7000 Disclosure of Information, 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls, 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, and 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. DFARS Clause 252.204-7000 restricts the release of unclassified *acquisition* information outside contractor's organization without prior Contracting Officer permission, with exceptions; DFARS Clause 252.204-7008 requires contractor compliance with Safeguarding Covered Defense Information Controls; DFARS Clause 252.204-7009 limits the use and disclosure of 3rd party cyber incident information; and DFARS 252.204-7012 requires contractor to provide adequate security for all covered contractor information systems (including implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" in effect at the acquisition is issued) and to comply with cyber incident reporting requirements.

2. Applicability. NAVFAC FE has determined that additional safeguards are essential for *acquisitions* where access to unclassified *NAVFAC FE information* marked **"CUI"** via an information system is required and/or where access to the same is provided to Offerors/Contractors or when such information may be generated by the same in response to such an *acquisition*. Offerors/Contractors must adhere to the OPSEC guidance stipulated below when receiving unclassified *NAVFAC FE information* marked to indicate the same must be safeguarded (e.g., "**CUI**")(see DoDI 5200.48) or when generating such information in response to an *acquisition* in order to protect the same and to avoid an OPSEC compromise or access to the same by unauthorized third parties including but not limited to an adversary (in order to maintain essential secrecy and/or for information security purposes). NAVFAC FE has determined that the OPSEC guidance stipulated below is required because this *acquisition* refers to and requires Offerors/Contractors to have access to unclassified *NAVFAC FE information* which has/have been marked **"CUI,"** in accordance with DoDI 5200.48.

CONTRACTOR DUTIES & RESPONSIBILITIES

(i) Offeror/Contractor shall limit disclosure of unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 within its own organization to its directors, officers, partners, members, and/or employees, collectively referred to as its affiliate(s), having a need to know.

(ii) Offeror/Contractor is required to provide *adequate security* for all unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 on *covered contractor information systems*.

(iii) It is recognized that *adequate security* will vary depending on the nature and sensitivity of the information on any given non-DoD information system. *However, all* unclassified *NAVFAC FE information* in the possession or control of non-DoD entities on non-DoD information systems shall minimally be safeguarded as follows:

a. Do not process unclassified *NAVFAC FE information* on publically available computers (e.g., those available for use by the general public in kiosks or hotel business centers).

b. Protect unclassified *NAVFAC FE information* by at least one physical or electronic barrier (e.g., locked container or room, logical authentication or logon procedure) when not under direct individual control of an authorized user.

c. At a minimum, overwrite media that have been used to process unclassified *NAVFAC FE information* before external release or disposal.

d. Encrypt all unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 when it is stored on mobile computing devices such as laptops and personal digital assistants, compact disks, or authorized removable storage media such as thumb drives and compact disks, using the best encryption technology available to the contractor or teaming partner.

e. Limit transfer of unclassified *NAVFAC FE information* to subcontractors or teaming partners with a need to know and obtain a commitment from them to protect the information they receive to at least the same level of protection as that specified herein, the contract or other written agreement.

f. Transmit e-mail, text messages, and similar communications containing unclassified *NAVFAC FE information* using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and transport layer security (TLS).

g. Encrypt organizational wireless connections and use encrypted wireless connections where available when traveling. If encrypted wireless is not available, encrypt document files (e.g., spreadsheet and word processing files), using at least application-provided password protected level encryption.

h. Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

i. Do not post unclassified *NAVFAC FE information* to website pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to website pages that control access by user identification and password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies during transmission. Access control may be provided by the intranet (vice the website itself or the application it hosts).

j. Provide protection against computer network intrusions and data exfiltration, minimally including:

(1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
(2) Monitoring and control of both inbound and outbound network traffic (e.g., at the external boundary, sub-networks, individual hosts), including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.
(3) Prompt application of security-relevant software patches, service packs, and hot fixes.

k. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, proprietary, critical program information (CPI), personally identifiable information, export controlled, etc.) as specified herein, in contracts, grants, and other legal agreements.

l. Report loss or unauthorized disclosure of unclassified *NAVFAC FE information* in accordance with the terms herein, the contract, grant, or other legal agreement requirements and mechanisms.

m. Do not use external IT services (e.g., e-mail, content hosting, database, document processing) unless they provide at least the same level of protection as that specified in the contract or other written agreement.

(iv) Offeror/Contractor's personnel shall not discuss unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 in public or over unprotected or unencrypted communications. *NAVFAC FE information* marked in accordance with DoDI 5200.48 may only be transmitted as directed by the Contracting Officer.

(v) Offeror/Contractor shall not transmit unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 electronically over the Internet unless it is encrypted in accordance with appropriate Federal regulations. If in doubt, contact the Contracting Officer.

(vi) Because specific restrictions are needed to preclude unintentional release of unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 to unauthorized parties including an adversary, unauthorized disclosure of the same may be punishable under 18 USC § 793 and/or any other applicable laws and/or regulations. Therefore, Offeror/Contractor's personnel shall not disclose to unauthorized third parties, post to unofficial sites (including Social Networking sites) any images, data or information related to unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48.

(vii) Unauthorized disclosure and/or attempts to solicit unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 by unauthorized third parties or others not affiliated with this *acquisition* shall be reported to the Contracting Officer, and/or the NAVFAC FE and/or installation Security Office, and your company Facility Security Officer and/or the Defense Security Service. **Non-Disclosure requirements remain in effect during the duration of the awarded contract for this acquisition and indefinitely thereafter.**

(viii) Practice OPSEC and implement countermeasures to protect unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48.

(ix) It is strongly recommended the Offeror/Contractor mark and protect related internal business information related to the *acquisition* and/or unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48. Internal company markings e.g., Business Sensitive, etc., are appropriate for identifying the aforementioned as sensitive information.

(x) Offeror/Contractor agrees to return or destroy unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 upon notice of award of a contract under this *acquisition* which required disclosure of said unclassified *NAVFAC FE information* or not later than 10 days after such award.

(xi) Offeror/Contractor agrees it shall identify all derivative works produced using unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48 to the Contracting Officer, not later than the above referenced date and request instructions on disposition or retention of such derivative works. A "derivative work," that is, a work that is based on (or derived from) one or more already existing works, in this case unclassified *NAVFAC FE information* marked in accordance with DoDI 5200.48.

(xii) Upon request by the Contracting Officer, Offeror/Contractor shall certify in writing or by email that he or she has destroyed the unclassified *NAVFAC FE information* within 10 days from such a request.

TERMS

Access – The ability or opportunity to obtain knowledge of controlled unclassified information.
Adequate security – means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
Adversary - Individuals, organizations, or countries that must be denied critical information in order to preserve mission integrity and maintain friendly mission effectiveness and the element of surprise. Adversary, in this context, includes any individual, organization, or country with which specific information should not be shared to preserve mission integrity or the element of surprise.
Covered Contractor Information System – means an information system that is owned or operated by a contractor that processes, stores, or transmits *Federal contract information*.
Controlled Unclassified Information (CUI) - Unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the United States Government (U.S. Government). It includes U.S. information that is determined to be exempt from public disclosure according to DoDD 5230.25, DoDD 5400.7, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). This includes FOR OFFICIAL USE ONLY, Unclassified-NNPI, and PII etc. or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list/.html).
Critical Information - Critical information is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it will prevent or seriously degrade mission success. Critical information can be classified information or unclassified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.
Critical infrastructure - Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health, or safety, environment, or any combination of these matters, across any Federal, state, regional, territorial, or local jurisdiction. **INCLUDES - Critical Energy Infrastructure Information**: specific engineering, vulnerability, or detailed design information about proposed or existing critical energy infrastructure that: (i) relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person planning an attack on critical infrastructure; … and (iii) Does not simply give the general location of the critical infrastructure.
Critical utility infrastructure - (e.g., electrical, water, gas, steam, communications, IT, security, industrial Control Systems): a. Inventory of IP-based control systems consisting of network capable digital controllers and user interfaces used to monitor and control equipment (i.e., building control systems, utility control systems, electronic security systems, and fire and life safety systems per DoDI 8500.01 and 8510.01); (b) user/password/media control addresses (MAC Address); and System logs, software and hardware configurations/operating systems (OS). **INCLUDES - DoD Critical Infrastructure Security Information** or information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities, including information regarding and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated on behalf of DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.
Federal Contract Information – means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments.
Essential Secrecy - The condition achieved from the denial of critical information to adversaries.
For Official Use Only (FOUO) - A designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). (A form of CUI)
Information – Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned, produced by or for, or is under the control of the U.S. Government.
Information system – means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 USC 3502).
Information security - The system of policies, procedures, and requirements established to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. The term also applies to policies, procedures, and requirements established to protect CUI, which may be withheld from release to the public in accordance with statute, regulation, or policy.
Need to Know - A determination that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function.
Recipient - Refers collectively to the Business or Company and its personnel (directors, officers, partners, members, and/or employees, collectively referred to as its affiliate(s)).
Operations Security - Operations security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems;
b. Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and
c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC compromise - The disclosure of critical information or sensitive information which has been identified by the Command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.
Procurement and Acquisition: material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, Federal contract information, indirect costs and direct labor rates.
Publicly Accessible web site - A Department of Defense (DoD) web site with access unrestricted by password or Public Key Infrastructure (PKI) user authorization. "Public" refers to the at-large audience on the Internet; anyone who can access a web site through a browser.

ADDENDUM "A"
CONTRACTOR OPSEC GUIDANCE

Public Release - The approved release of coordinated, consistent, accurate, and authoritative information that meets appropriate security regulations and Navy/DoD guidelines for the release of information to the public. The NAVFACFE Public Affairs Officer is the point of contact for all Public Release material.
Safeguarding - Measures and controls that are prescribed to protect classified and/or controlled unclassified information and/or information systems.
Security Manager - A properly cleared individual having professional security credentials to serve as the manager for an activity.
Sensitive Information - Sensitive information is information requiring special protection from disclosure that could cause compromise or threat to our national security, a Navy organization, activity, family member, DoD civilian or DOD contractor.
Social Media - Refers to the means of interactions among people in which they create, share, and exchange information and ideas in virtual communities and networks; Facebook, Twitter, LinkedIn, etc.
Solicitation – Refers to a Request for Proposal (RFP) Request for Quote (RFP) and/or Invitation for Bod (IFB).
Unclassified Information - Information that may be sensitive in nature, is not classified by nature. Unclassified information is NOT releasable to the public without public release authority of the information owner.

REFERENCES

(a) National Security Decision Directive Number 298, National Operations Security Program (Jan 22, 1988)
(b) DoDD 5205.02E, Department of Defense Operations Security (OPSEC) Program (May 11, 2018)
(c) OPNAVINST 3432.1A, Operations Security (August 4, 2011)
(d) NAVFACINST 3070.2, Naval Facilities Engineering Command, Operations Security (06 NOV 2017)
(e) NAVFACFEINST 3432.1, Operations Security (24 AUG 2017)
(f) U.S. Navy NTTP 3-13.3M, U.S. Marine Corps MCTP 3-32B, Operations Security (SEP 2017)
(g) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"
(h) DoDD 5230.09 Clearance of DoD Information for Public Release (Jan 25, 2019)
(i) DoDM 5200.01, Vol 1-3 "DoD Information Security Programs (Feb 24, 2012)(Incorporating Change 1, Effective May 9, 2018)
(j) DoDI 5200.48, "Controlled Unclassified Information" (CUI)(06 Mar 2020)
(k) DoDI 8500.01 Cybersecurity (March 14, 2014)
(l) DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling (May 24, 2011)
(m) DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems (June 6, 2012)(Incorporating Change 1, October 27, 2017)
(n) DoDI 5230.24 Distribution Statements on Technical Documents (Oct 15, 2018)
(o) Federal Acquisition Regulations (FAR) 4.19 Basic Safeguarding of Covered Contractor Information Systems and 52.204-21 Basic Safeguarding of Covered Contractor Information Systems
(p) Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 204.404-70 Additional contract clauses, 204.7301, 204.7303 Definitions, 204.7303 Procedures, PGI 204.7303; Solicitation provisions and contract clauses; 252.204-7000 Disclosure of information, 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls, 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, and 252.204-7012 Safeguarding Covered Defense Information And Cyber Incident Reporting