OPERATIONS SECURITY PLAN FOR CONTRACTORS

Tracking Number

U-23-59

PRINT CLEARLY

1. NAME OF CONTRACTOR COMPANY

2. CONTRACTOR COMPANY ADDRESS

3a. NAME OF PHNSY&IMF REQUIRING ACTIVITY REPRESENTATIVE **3b. CODE** **3c. IP NUMBER**

4. TODAY'S DATE **5. PERFORMANCE START DATE** **6. PERFORMANCE END DATE**

OPERATIONS SECURITY (OPSEC) STATEMENT

This OPSEC plan is used to record, identify and monitor the contractor's OPSEC activities during the performance of this contract. After award but prior to availability start date, this OPSEC plan must be signed by the Prime contractor and forwarded to the assigned contracting official by encrypted email, through the approved Department of Defense Safe (DoD) Secure Access File Exchange (SAFE) at https://safe.apps.mil, or by United States Postal Service. **THIS FORM SHALL BE PROTECTED FROM PUBLIC RELEASE.**

DISTRIBUTION AND WARNING STATEMENT

Federal Employees and Contractors Only: Distribution authorized to DoD and DoD US contractors only for Operations Security. Includes individuals or employees who enter into a contract with the U.S. to perform a specific job, supply labor and materials, or for the sale of products and services, so long dissemination is in furtherance of the contractual purpose.

Warning: This document may contain technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751 et seq.) or Executive Order 12470. Violation of these export laws is subject to severe criminal penalties.

Controlled Unclassified Information (CUI) - The information contained in this document and any accompanying attachments may contain information which is protected from mandatory disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. 552.1.

REFERENCES

- DoDM 5205.02, Operations Security Program Manual, 3 November 2008

PH-SYD IMF 3070/2

Controlled by: DON, PHNSY&IMF
Controlled by: [redacted]
CUI Category: OPSEC
Distribution/Dissemination: FEDCON
POC: [redacted]

CONTRACT NUMBER: _____

OPSEC REQUIREMENTS

All contractors and subcontractors will accomplish the following minimum requirements in support of Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility (PHNSY&IMF) OPSEC Program.

1. Applicability. This OPSEC Plan applies to contractors conducting sensitive work whether classified or unclassified onboard PHNSY&IMF.

2. OPSEC Process. OPSEC is a process used to protect sensitive information from exploitation by an adversary. Sensitive information, which is also referred to as Critical Information (CI) is defined as information that needs to be protected from unauthorized disclosure.

3. What is CI? CI is sensitive information whether classified or unclassified which must be protected from loss to keep an adversary from gaining a significant operational, economic, political or technological advantage and prevent adverse impact on the Shipyard's mission accomplishments.

4. The OPSEC process is most effective when fully integrated into all planning and operational processes. The OPSEC process involves five steps:

    a. Identify CI – Determine what information must be protected? Why do you want to protect it?

    b. Analyze the Threat – Who wants it, who is your adversary?

    c. Analyze Vulnerabilities – How can an adversary obtain this information? How can we protect it?

    d. Assess the Risk – How will this impact your mission if exploited?

    e. Apply countermeasures – Reduce your weaknesses. Ensure to follow procedures that are in place.

5. Adherence to this OPSEC Plan is the responsibility of Prime contractor.

    a. The Prime contractor will coordinate the implementation of training, administration, and execution and ensure all procedures identified in this plan are followed.

    b. All contractors and subcontractors are responsible for the successful implementation of this plan.

    c. PHNSY&IMF Security will support the supporting contracting company in the development, implementation and compliance with security procedures established in the s OPSEC plan.

    d. Contractor personnel to this contract shall utilize this plan to protect all CI.

JOB DESCRIPTION

CONTRACT OBJECTIVE. *Place a brief description of job procurement or job work below. This includes unclassified work.*
- If the contract requires access to classified information or material, detailed security requirements shall be in accordance with DD Form 254. Refer to block 9 of the DD 254 for job work.

e.g. The specific objective of this contractual effort is to provide PHNSY&IMF with _____

CONTRACT NUMBER: _____

COMPLIANCE ON WHAT SENSITIVE INFORMATION TO PROTECT (BUT NOT LIMITED TO)

During the period of this contract, contractor personnel may be exposed to, use, or produce, U.S. Government CI and observables indicators which may lead to discovery of CI. Paragraphs in this section shall be controlled and will not be distributed to unauthorized third parties, including foreign governments, or Foreign Ownership, Control, or Influence (FOCI) companies.

a. No classified or unclassified Naval Nuclear Propulsion Information (NNPI) material will be removed from any shipyard space or ships in the performance of this contract unless approved in writing by the PHNSY&IMF Command Security Manager (CSM). Description, drawings, technical papers, components, or equipment designed specifically for specialized production must be controlled and safeguarded at all times. This also includes names and personal information, including Personal Identifiable Information (PII) of company and government employees.

b. The contractor shall not post classified information or CUI to company websites, publications, newsletters or other media, any images, data or information that reveal sensitive government operations, personnel, or equipment details. In addition, tactics, techniques and procedures; production or work schedules; any visible or concealed modifications, upgrades, additions to vessel, weapons or equipment; increases, changes, or decreases in work or deployment frequency and vessel movements.

c. The contractor and its personnel shall not divulge any information about files, data processing activities or functions on public social media sites or to personnel who do not have a need to know.

d. Government issued badges, identification shall be removed and/or concealed from plain sight when off PHNSY&IMF and shall not be left in vehicles or unprotected. Badges and passes may not be duplicated, copied or loaned to others. Lost or stolen identification badges, vehicle passes, etc., will be immediately reported to requiring representative, PHNSY&IMF Security Office and the Joint Base Pearl Harbor-Hickam (JBPHH) Police Department. (Upon completion of this contract, the Contractor and all assigned to this contract will return (i.e., all access badges, passes, keys) before leaving PHNSY&IMF premises).

COUNTERMEASURES ON HOW TO PROTECT SENSITIVE INFORMATION (BUT NOT LIMITED TO)

The Contractor shall protect all CI as stated throughout this plan in a manner appropriate to the nature of the information.

a. Practice OPSEC and maintain Security Awareness at all times.

b. Restricting verbal discussion of CI to venues and circumstances that prevent the monitoring and interception of the discussion by unauthorized personnel

c. The Contractor may work with internal production schedules, deliverables, and inventories. The Contractor shall safeguard this information from disclosure, inadvertent or otherwise, from unauthorized recipients.

d. Immediately and appropriately, destroy all CI no longer needed under this contract requirement. Documents will be destroyed via National Security Agency (NSA) approved product listed crosscut shredders or disintegrators that are capable of rendering the documents unrecognizable and makes it difficult to reconstruct.

e. Do not throw any shipyard related documents in the trash.

CONTRACT NUMBER: _____

PHNSY&IMF CAMERA - PERSONAL ELECTRONIC DEVICE (PED) POLICY

• Personal photography is prohibited in PHNSY&IMF, to include personal cellular phones with camera features.

• When operationally required, a written request containing specific justification and details will be submitted to the PHNSY&IMF Command Security Manager via the Government Contracting Activity for consideration.

• Personal electronic devices (PEDs) include, but are not limited to: pagers, mobile/cellular telephones (with/without cameras), personal digital assistants/job performance aids, laptop/notebook/handheld computers, digital imagery (still/video) devices, analog/digital sound recorders (e.g. I-PODs), Fit-Bits, I-Watches, video game devices, USB devices, and devices of similar capability, functionality, or design. These devices are controlled and their use is dependent upon Shipyard guidance. Before use, coordinate with your sponsor, who can assist you by obtaining and sharing these requirements/controls with you. It is expected that if additional guidance is needed, the sponsor will coordinate with PHNSY&IMF Computer Security division and determine what can be used and what is prohibited. Failure to do so risks security violations for the holder of the device.

• Contractor personnel shall not share written content, take photographs, or make any recordings (audio, visual digital) in the performance of this contract unless approved in writing by the PHNSY&IMF CSM.

• Contractor personnel shall not enter PHNSY&IMF spaces, Controlled Industrial Area (CIA), Controlled Nuclear Information Area (CNIA), or Nuclear Work Areas (NWA) or any other restricted area with personal electronic devices, laptops, tablet PCs, cellular phones, cameras, recording devices, and data recording/storage devices, unless prior authorized.

COMPUTER NETWORK USE

Contractor may request access to PHNSY&IMF information systems based on the requirement of the contract. Contractor employees must successfully complete Cyber Awareness and OPSEC training, and submit with their information system access request. **Ensure you provide training certificates to your shipyard sponsor.**

Cyber Awareness – https://public.cyber.mil/training/cyber-awareness-challenge/

OPSEC – https://securityawareness.usalearning.gov/opsec/index.htm

CUI REQUIREMENTS FOR CONTRACTORS

This paragraph highlights requirements for contractors.

a. Contractors involved with CUI in pursuant to contractual requirements must:

Complete CUI training prior to arrival. Certificates must be provided to the OPSEC PM prior to arrival. https://securityawareness.usalearning.gov/cui/index.html.

COMPROMISE - UNAUTHORIZED DISCLOSURE

OPSEC compromise is the disclosure of CI or sensitive information that 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 equipment. The Contractor and all subcontractors under this contract will understand the following:

CONTRACT NUMBER: _____

a. The Contractor and its personnel shall realize that disclosure or compromise of CI to unauthorized persons, whether willfully or through gross negligence, carelessness, or indiscretion, may warrant action to remove the individual assigned or to terminate contract.

b. Contractor and its personnel can be for the purpose of conducting any investigation of alleged misconduct, which may, in the opinion of the Contracting Officer, jeopardize the security of the project. Whenever there is probable cause to believe that such action is warranted in the interest of national security.

c. Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss or compromise of government CI related to this contract shall be immediately reported to the PHNSY&IMF CSM or the JBPHH Naval Criminal Investigation Service (NCIS).

d. Non-Disclosure requirements remain in effect during the duration of this contract and indefinitely thereafter.

PRIME CONTRACTOR CONCURRENCE

A determination to request access and conduct work for PHNSY&IMF is a matter of inherent command authority. Please following requested requirements.

a. Contractors shall not have access to sensitive information unless it is required for them to accomplish the tasks required in the contract.

b. The Prime contractor must submit this signed OPSEC Security Plan prior to contract award.

c. The Contractor and subcontractors shall ensure that its personnel supporting PHNSY&IMF comply with all measures outlined in this plan.

d. The Contractor shall institute and implement all effective OPSEC measures to prevent any violations by its employees and subcontractors.

e. The Prime Contractor will be responsible for the identification and protection of the identity of personnel working in support of this mission. This includes all contractors and subcontractors names, addresses and other contact information.

f. The Prime Contractor POC must sign the bottom of this plan stating, "*Contractor and all subcontractors under this contract will review this document and will become familiar with the guidance detailed in this plan and the OPSEC process.*"

PRIME CONTRACTOR POC	
a. NAME	b. SIGNATURE
c. EMAIL	d. PHONE
e. TITLE	