Norfolk Naval Shipyard
Operations Security (OPSEC) Contract Requirements

Attach with Solicitation and Award

Reference

DoDM 5205.02, Operations Security Program Manual, 3 November 2008

What is OPSEC?

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 whether classified or unclassified.

What is an OPSEC Plan?

An OPSEC plan is used to record, identify and monitor the contractor's OPSEC activities during the performance of the 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.

Consideration shall be given depending on the type of work being performed, the environment, and circumstances in which contract performance will occur. In some cases, an OPSEC Plan will be required. In other cases, the contractors may only simply be required to receive this basic OPSEC contract requirements form.

☑ OPSEC Plan is required. Refer to OPSEC Plan for Contractors (separate attachment).
☐ OPSEC Plan is NOT required.

Responsibility of the Contractor

It is the responsibility of all contractors and subcontractors to avoid inadvertent disclosure of unclassified or classified information during the period of this contract.

OPSEC compromise is the disclosure of Critical Information (CI) or sensitive information, which has been identified by the Command and any higher headquarters to adequately protect its personnel and equipment.

During the period of this contract, contractor personnel may be exposed to, use, or produce, U.S. Government CI and observable indicators which may lead to disclosure of CI. NNSY CI will not be distributed to unauthorized third parties, including foreign government or companies under Foreign Ownership, Control or Influence (FOCI). The contractor shall protect all CI in a manner appropriate to the nature of the information.

U.S. Government CI shall not be publicized in corporate wide newsletters, trade magazines, displays, internet page or public websites. All transmission to personal email accounts (AOL, Yahoo, Gmail, Hotmail, Comcast, etc.,) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.,) is prohibited. Media requests related to this project shall be directed to NNSY Public Release Authority.

The Contractor and its personnel should 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. Furthermore, such conduct may be cause for criminal prosecution and imposition of criminal and civil penalties.

Protect Controlled Unclassified Information (CUI): Unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy. Any attempt by unauthorized third parties to solicit, obtain, photograph or record incidents of loss or compromise of CUI or other pertinent sensitive

OPSEC Contract Requirements (cont)

information related to this contract shall be immediately reported to the organization's Command Security Manager Code 1127 and the Information & Industrial Security Branch Code 1122.

NNSY Portable Electronic Device (PED) Policy

Portable 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 NNSY 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.

OPSEC Critical Information and Indicator List, including Countermeasures

Critical Information is an adversary's target of choice. Seemingly, harmless UNCLASSIFIED data with other conversations, presentations, emails or documents could reveal classified information.

THREAT/RISK	COUNTERMEASURES
EXAMPLES OF OUR CRITICAL INFORMATION ARE, BUT NOT LIMITED TO:	**EXAMPLES OF OUR COUNTERMEASURES, BUT NOT LIMITED TO**
• PERSONALLY IDENTIFIABLE INFORMATION (PII) – INFORMATION ABOUT AN INDIVIDUAL THAT IDENTIFIES, LINKS, RELATES, OR IS UNIQUE TO, OR DESCRIBES INDIVIDUALS, FOR EXAMPLE, SOCIAL SECURITY NUMBER, AGE, HOME ADDRESS, PERSONAL PRIVACY ISSUES, DEMOGRAPHIC, MEDICAL STATUS, AND IDENTIFIERS COVERED BY PRIVACY ACT.	**• Contractor shall not post classified information or Controlled Unclassified Information (CUI) to company websites, publications, newsletters or other media, images, data or information that reveal sensitive government operations, personnel, or equipment details.**
• RESTRICT VERBAL DISCUSSION REGARDING NNSY SHIPYARD RELATED WORK.	**• Shred ALL sensitive information, CUI and other pertinent critical information when no longer needed. Do not throw any shipyard related documents in the trash. Use the approved NSA crosscut shredders assigned.**
• OPERATION SCHEDULE, SHIP REPAIR SCHEDULE, DRILL AND SUBMARINE DOCKING SCHEDULES.	**• *DO NOT* post shipyard related information on public social media websites.**
• EQUIPMENT CAPABILITIES, LIMITATIONS AND VULNERABILITIES.	**• Remove issued badges when you leave the shipyard, including lunch hours. Upon completion of contract, return all access badges, passes, keys before leaving NNSY premises. Badges and passes may not be duplicated, copied or loaned to others. Lost or stolen identification badges must be reported immediately.**
• IDENTIFICATION OF SPECIFIC ASSETS, FACILITIES, SYSTEMS, AND NETWORKS CRITICAL INFRASTRUCTURE.	**• Report any unauthorized disclosure or, known and suspected compromises of critical information immediately to the unit sponsor, prime contract officer and the units Command Security Manager.**
• RESTRICT PHOTOGRAPHS, IMAGES AND VIDEOS TAKEN WITHIN ANY SHIPYARD WORK AREAS, TO INCLUDE DRYDOCKS, SHIPS, RESTRICTED AREAS AND CONTROLLED ACCESS AREAS.