

**Naval Air Warfare Center Weapons Division (NAWCWD)
Operations Security (OPSEC) and Critical Information Annex**

1. All work is to be performed in accordance with Department of Defense (DoD), and Department of the Navy (DON), Operations Security (OPSEC) requirements, per the following:
 - a) National Security Decision Directive 298
 - b) DoDD 5205.02E, DoD Operations Security (OPSEC) Program
 - c) DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual
 - d) OPNAVINST 3432.1A, DON Operations Security
 - e) SECNAVINST 3070.2A, Operations Security
 - f) NTTP 3-13.3M/MCTP 3-32B, Operations Security
 - g) Joint Publication 3-13.3, Operations Security
2. The contractor shall accomplish the following minimum requirements in support of the NAWCWD OPSEC Program:
 - a) Determine Critical Information (CI) in accordance with DoDM 5205.02 (Appendix 1 through Enclosure 3). Critical Information, which individually, or in aggregate, reveal sensitive details about NAWCWD or the contractor's security or operations.
 - b) Adhere to OPSEC Measures and implement countermeasures to protect CI and sensitive activities, especially information or activities that could compromise classified information, operations, or degrade the planning and execution of operations performed or supported by the contractor, and or subcontractors in support of the mission.
 - c) NAWCWD has identified the following baseline Critical Information and Indicators List (CIIL):
 - 1) Details regarding military operations, missions and exercises
 - 2) System and Program Tactics, Techniques and Procedures
 - 3) Emergency response procedures, capabilities, rally points and recall procedures
 - 4) Measures used in Force Protection Conditions (FPCON), and Standard Operating Procedures (SOP)
 - 5) Operational characteristics for new or modified weapon systems
 - 6) Test or evaluation information pertaining to events, scheduling, dates and times
 - 7) Known or probable vulnerabilities to any weapon system or their support systems
 - 8) Intelligence sources or methods of gaining intelligence
 - 9) Information revealing communications security (COMSEC), TEMPEST or Physical Security vulnerabilities
 - 10) Communications systems status, upgrades or proposed changes
 - 11) Network user identifications (IDs), passwords and access codes to restricted/controlled spaces
 - 12) Travel reservations and plans, locations, routes and VIP agendas
 - 13) Personnel privacy: Names, phone numbers, addresses, financials, job titles and passwords
 - 14) Increased/decreased budget costs for future force or mission changes

All CI developed by the contractor and or NAWCWD in electronic or hard-copy form shall be protected by a minimum of the following countermeasures:

CI may not be discussed via non-secure phones

CI may not be provided to individuals that do not have a "need-to-know"

3. If the contractor cannot resolve an issue concerning OPSEC Measures, they will contact the Contracting Officer's Representative (COR), who shall consult with the appropriate NAWCWD Security Officer, Security Coordinator, or Technical Point of Contact (TPOC).

CRITICAL INFORMATION

1. Critical Information (CI) is specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Left unprotected, Critical Information provides unclassified evidence of the planning and execution of sensitive command activities. Critical Information includes otherwise unprotected technology development, application, RDT&E information and sensitive information; providing adversaries with insight on mission activities, e.g., parts ordering, prime and subcontractor communications, test and evaluation, and shipping of deliverables.
2. The Department of the Navy (DON) maintains a DON Critical Information and Indicators List (CIIL), described in the Navy Tactics, Techniques and Procedures (NTTP 3-13.3M). The DON CIIL informs the command CIIL, the NAWCWD CIIL shall be employed in determining command CI and OPSEC posture.
3. The commands identified CI is maintained in the CIIL, approved by the NAWCWD Commander, that outlines command information that while unclassified, requires protection from compromise or unauthorized disclosure. The approved command CIIL is coordinated and maintained by the NAWCWD OPSEC Officer. Programs Projects and Organizations (PPO) will identify Critical Information specific to their activities, and or procedures and measures for their protection. PPO specific Critical Information will be added to the command CIIL for an all-inclusive CIIL, and shall be posted at all (NAWCWD) employee workstations.
4. Inclusion in the command CIIL in and of itself does not classify the information or preclude the information from public release. Public Affairs and the OPSEC Officer shall work with command leadership to determine what level of detail to release publicly when information identified on the command CIIL is desired for public release. Generally however, and until approved for public release by command leadership, information on the approved CIIL will not be released publicly and will not be discussed over non-secure phones or in public areas.
5. Critical information shall be transmitted in a manner that reduces the risk of aggregation and compromise. Where practicable, a classified network (either data or phone) is the preferred method of transmission for critical information. When a classified network is not available and the information is not sensitive to ongoing or planned operations, then it may be transmitted over an unclassified network so long as it is encrypted. Unencrypted transmission of critical information over an unclassified network is not authorized.