RMKS/1. Operations Security (OPSEC) and the requisite protection of critical information are priorities for the Department of the Navy (DON). SECNAVINST 3070.2, Operations Security, was issued 5 May 2016. This new policy requires the implementation of effective OPSEC programs and additional measures to protect critical information. The instruction can be obtained from the DON Issuance webpage: (https://doni.dla.mil/Directives/03000%20Naval%20Operations%20and%20Readiness/03-00%20General%20Operations%20and%20Readiness%20Support/3070.2.pdf). This guidance should receive wide dissemination, but is of particular importance to Public Affairs, Information Warfare, Acquisition, Antiterrorism/Force Protection (ATFP), and security professionals.

2. Current threats require that we redouble our efforts to protect critical information through enhanced collaboration between OPSEC program managers, command security offices, Public Affairs specialists, the Information Warfare community, ATFP personnel, and other security professionals. Exploitation of internet based capabilities, publicly released information, and other UNCLASSIFIED but potentially sensitive data gives adversaries the ability to undermine our technological edge, threaten our personnel, and potentially compromise our operations.

3. Key elements of the policy:
   a. OPSEC is explicitly the responsibility of each Commanding Officer or equivalent.
   b. OPSEC must be considered and incorporated into all operational planning and execution.
   c. A requirement for commands to develop, resource, and maintain effective OPSEC programs.
   d. OPSEC is clearly defined as an Operations rather than a Security function.
   e. It enhances accountability and requirements for all higher commands to provide oversight of subordinate OPSEC programs.
   f. Failure to attain mandated standards shall result in disqualification from all operational awards.
   g. Requirement for incorporation of OPSEC into the entire Research, Development, Test and Evaluation life cycle.
h. Documented OPSEC training is a pre-requisite for access to all DON information systems.
   i. Each Command shall develop and implement enforcement mechanisms to reduce disclosures of critical information per SECNAVINST 3070.2 (Enclosure 2).
   j. OPSEC requires continuous collaboration between ATFP personnel, public affairs specialists, command security professionals, and OPSEC program managers.
   k. A requirement for OPSEC to be a stand-alone mission essential task and not subordinated under other readiness qualification criteria (e.g., Electronic Warfare and Information Operations). Additionally, OPSEC is required to be incorporated into all assess-train-certify related documentation and requirements.
   l. Evaluation of every solicitation/contract award package to ensure OPSEC requirements are met in accordance with each Commands OPSEC policy. OPSEC requirements should be assessed for inclusion in all DD Form 254.

4. For the Navy, while the new policy requires O-3/GS-12 program managers, per this ALNAV, a waiver is automatically granted for warfare qualified Information Warfare officers CWO-2 and above at commands below the Echelon II level.

5. OPSEC resources:
   a. An OPSEC self-inspection tool, included as part of the policy, facilitates an internal assessment of compliance with Department of Defense and DON standards and provides higher level commands the ability to evaluate the effectiveness of subordinate programs.
   b. The DON Critical Information List (CIL) provides an overview of what the Secretary of the Navy (SECNAV) considers critical information across the Department. A DON-wide CIL is also included in the policy.
   c. The Naval OPSEC Support Team, which can be reached via http://www.Facebook.com/NavalOPSEC, the OPSEC link on the Navy Homepage, or by e-mailing the team at opsec@navy.mil.
   d. The Marine OPSEC Support Team can be reached via the OPSEC link on the Marine Corps Information Operations Command Homepage or by emailing the team at OPSEC@usmc.mil.
   e. The Naval OPSEC application (APP), an excellent tool for OPSEC program managers, Marines, and Sailors, provides access to resources and policies, training links, videos and various products, as well as the ability to complete annual OPSEC general military training. The APP is available in the Apple App Store and Google Play Store under the title Naval OPSEC.

6. In light of the current threat environment, existing guidance on the release of personally identifiable information (PII) of DON personnel was reviewed. Most types of personal information are already included in the DON CIL. Much personal information, including association with military and government entities, is already in the public domain (e.g., many names and associated services). Per reference (a), SECNAV may withhold normally releasable PII (e.g., names and associated command) based on specific credible changes to the threat environment. This authority cannot be delegated. Director, Naval Criminal Investigative Service (NCIS) will determine the credibility of the threat. Chief of Naval Operations and/or Commandant of the Marine Corps, based on NCIS determination, in coordination with Navy Chief of Information, will make recommendations to SECNAV on the nature and scope of proposed restrictions. Any restrictions should be short in duration and relaxed immediately upon NCIS determination that the relevant threat is no longer viable.
7. Deputy Under Secretary of the Navy (Policy) OPSEC point of contact is LCDR Josh Segal. He can be reached at joshua.e.segal@navy.mil.

8. SECNAVINST 3070.2, signed 5 May 2016, shall be implemented immediately, and its guidance supersedes current service-level direction until revised policies are promulgated bringing them into compliance with current department level policy.

9. Released by Ray Mabus, Secretary of the Navy.//

BT
#0001
NNNN
UNCLASSIFIED//