DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

20 May 2014

MEMORANDUM FOR DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION OFFICER (NAVY)
DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION OFFICER (MARINE CORPS)

Subj: DON IMPLEMENTATION OF THE RISK MANAGEMENT FRAMEWORK (RMF) FOR DOD INFORMATION TECHNOLOGY (IT)

Ref: (a) DoD Instruction 8510.01 of 12 March 2014, Risk Management Framework (RMF) for DoD Information Technology (IT)
(b) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Guide for Applying the Risk Management Framework to Federal Information System of February 2010, as amended
(c) Committee on National Security Systems Instruction 1253 of March 27, 2014, Security Categorization and Control Selection for National Security Systems as amended
(d) NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, of 30 April 2013, as amended
(e) DoD Instruction 8500.01 of 14 March 2014, DoD Cybersecurity

The purpose of this memorandum is to implement the Risk Management Framework (RMF) for DoD Information Technology (IT), reference (a), within the Department of the Navy (DON). RMF implementation includes the framework in reference (b), the system categorization method and baseline security control sets in reference (c), and the catalog of security controls in reference (d). Per reference (a) and in accordance with reference (e), Components have been given six months to begin using the RMF for DoD IT.

The DON Senior Information Security Officer (SISO), formerly Senior Information Assurance Officer (SIAO), is appointed by the DON Chief Information Officer (CIO) and is responsible for implementing, overseeing, and enforcing the RMF and ensuring the quality, capacity, visibility, and effectiveness of the RMF for DoD IT process within the DON. The SISO is further designated as the Security Control Assessor (SCA) (formerly Certifying Authority (CA)), with responsibility for system risk assessment. The SISO may delegate the security control assessment responsibilities of the SCA role for governed IT, but may not delegate process oversight.

The DON CIO will retain the SISO position at the Secretariat level in order to maintain proper oversight and ensure continuity between the Navy and Marine Corps, but will delegate SCA responsibilities. The Services are to submit their SCA nominations within 30 days of this

memorandum. Nominations are to include:

- Names of persons or teams, including an assurance that all delegates will meet cybersecurity workforce requirements.
  - An acknowledgement that the SCA(s) will not delegate the assessment duties any further.
  - Plans for standardizing and documenting the assessment review process.

The Navy and Marine Corps RMF implementation plans are due to the DON SISO for review by 1 July 2014. The Service RMF plans will use common definitions and processes to the fullest extent possible and will include:

- An approach for authorizing all DoD IT as identified in references (a) and (e).
- Justification for any Service specific additions to DoD requirements.
- A Navy/Marine Corps joint authorization process for systems deploying to both Services.
- Plans for active engagement with stakeholders of expiring systems and tracking of all system plan of action and milestones (POA&M) action items, including each DON Deputy CIO's plan for ensuring expiring systems' continued compliance.
- A minimum baseline assessment for annual reviews.
- A high risk escalation process wherein initial approval by the DON Deputy CIO is for no longer than six months and subsequent escalations must be submitted to DON CIO via the appropriate DON Deputy CIO. Each Service must maintain a minimum of 95 percent of its total systems as authorized to operate. Failure to maintain this minimum may result in a Service losing authorized actions for initial high risk escalations.
- Innovative and cost effective mitigation techniques to address high risk systems prior to escalation.

Each RMF plan will also contain a Configuration Management (CM) Plan that describes the Service's process for approving authoritative information and identifies where authoritative information is published. Additionally, the CM Plan will define methods for quickly identifying needed clarifications or minor changes; describe how notice of intent to publish changes will be publicized prior to implementation; and provide a means for documenting stakeholder recommendations for the Service's RMF implementation.

Once the SCAs are appointed and the RMF plans approved, the Services may make minor updates to their processes, but substantial changes or added requirements will require DON SISO approval. The DON CIO point of contact is Mr. Shaun Khalfan, 703-695-2927, shaun.khalfan@navy.mil.

Terry A. Halvorsen
Department of the Navy Chief Information Officer

Copy to:
CNO
CMC