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

3 December 2013

MEMORANDUM FOR DISTRIBUTION

Subj: DEPARTMENT OF THE NAVY (DON) POLICY FOR APPROVING MULTIFUNCTIONAL DEVICES (MFD) FOR USE ON DON NETWORKS

Ref: (a) DoD Instruction 8500.2, Information Assurance (IA) Implementation, of Feb 6, 2003
(b) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of November 28, 2007
(c) DON CIO Memo, Mandatory Guidance Regarding Management of Department of the Navy Copiers, Printers, Fax Machines, Scanners, and Multifunctional Devices, of January 25, 2013
(d) Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), Multifunction Devices and Network Printers (The current approved version)

The purpose of this memorandum is to facilitate the Department of the Navy's (DON) Multifunctional Device (MFD) efficiency initiative. The DON requires a process that allows competitive pricing and timely approval of MFDs while maintaining the security of DON networks and compliance with references (a) and (b). The DON must also minimize the administrative level of effort involved in adding an MFD to an accredited environment. This memo provides guidance for connecting MFDs purchased in accordance with reference (c) to DON networks.

MFDs can present significant vulnerabilities if not properly configured. Program Management Offices (PMOs) or commands may field MFDs using the system, enclave, or site current certification and accreditation (C&A), provided the following actions are taken:

- Configure the devices and the hosting environment in accordance with reference (d) and other applicable hardening guidance to ensure the devices are Information Assurance Vulnerability Management (IAVM) compliant and configured in accordance with Department of Defense IA requirements.
- Upload the compliance results in accordance with reference (d) into the appropriate C&A tool under the already accredited system, enclave, or site package. There is no time limit on the Security Technical Implementation Guide (STIG) compliance results; however, the Program must evaluate for impact any new STIG requirements that DISA has published since the original STIG compliance validation. The PMO or command must also close all CAT I findings and close or mitigate all CAT II findings; mitigations must be approved by a fully qualified Validator.

- Update the existing C&A package diagrams, system/network hardware/software lists and Ports, Protocols, and Services (PPS).
- Create a plan of action and milestones (POA&M) entry in the affected network's authorization documentation to investigate Common Criteria approval. The appropriate Validator-assigned residual risk must be included.

The PMO or command deploying the MFD must ensure the device remains STIG and IAVM compliant throughout its life cycle.

The DON point of contact for this matter is Dan DelGrosso, (703) 695-2900 or dan.delgrosso@navy.mil .

Terry A. Halvorsen
Department of the Navy
Chief Information Officer

Distribution
CNO
CMC
ASN (RD&A)
ASN (FM&C)
ASN (M&RA)
ASN (EI&E)
DON/AA
DUSN/DCMO
DUSN (PPOI)
OPNAV (DNS, N2/N6)
HQMC (C4, I&L)
PEO (A)
PEO (T)
PEO (U&W)
PEO Carriers
PEO C4I
PEO EIS
PEOIWS
PEO JSF
PEO LS
PEO LCS
PEO Ships
PEO Space
PEO Subs
DASN (C41 & Space)

Distribution: (continued)
COMPACFLT
COMUSFLTFORCOM
COMUSNAVEURUSNAVAF
CNIC
USNA
NAVWARCOL
NAVPGSCOL
COMUSNA VCENT
COMFLTCYBERCOM
COMNAVAIRSYSCOM
COMNAVSEASYSCOM
COMNAVSUPSYSCOM
COMUSNAVSO
COMNAVFACENGCOM
COMNAVSPECWARCOM
COMSPAWARSYSCOM
DIRSSP
BUPERS
COMNAVDIST
ONI
FLDSUPPACT
COMOPTEVFOR
NAVIOCOM
COMMARCORSYSCOM
MARFORCYBER