



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 ELECTRONIC FINGERPRINT (EFP) SOFTWARE AND HARDWARE FOR USE ON DON NETWORKS

- Ref: (a) DoD Memo, DoD Transition to Electronic Fingerprint Capture and Submission in Support of Background Investigations, of July 29, 2010
(b) DoD Instruction 8500.2, Information Assurance (IA) Implementation, of Feb 6, 2003
(c) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of November 28, 2007
(d) Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), Multifunction Devices and Network Printers (The current approved version)

The Department of the Navy (DON) requires a process that allows timely Approval to Operate (ATO) for end-user electronic fingerprint (eFP) hardware and software on DON networks to support the DON's efficiency efforts and to meet the 31 December 2013 deadline to transition to electronic capture and submission of fingerprint images prescribed in reference (a). This memorandum outlines an efficient path to compliance with DoD information systems Certification and Accreditation (C&A) requirements (references (b) and (c)) when connecting end-user eFP hardware and installing end-user eFP software on DON networks.

eFP hardware and software can present vulnerabilities if not properly configured. Program Management Offices (PMO) or commands may field eFP hardware and software using the current system, enclave, or site C&A when the following conditions are met:

- The eFP software (correct version) must be registered and approved in the DON Application and Database Management System (DADMS).
- All eFP hardware and software must be on the Federal Bureau of Investigation certified products list and must support all features and functions necessary for successful transmission to the Office of Personnel Management (OPM).
- The devices and hosting environment must be configured in accordance with reference (d) and must ensure the devices are Information Assurance Vulnerability Management (IAVM) compliant.
- The compliance results must be uploaded in accordance with reference (d) into the appropriate C&A tool under the already accredited system, enclave, or site package. Security Technical Implementation Guide (STIG) compliance does not expire; however, the Program must evaluate any new requirements that DISA has published since the

Subj: DEPARTMENT OF THE NAVY (DON) POLICY FOR APPROVING ELECTRONIC FINGERPRINT (EFP) SOFTWARE AND HARDWARE FOR USE ON DON NETWORKS

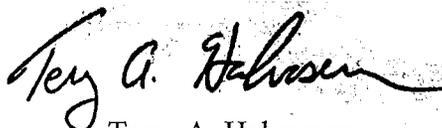
original STIG compliance validation. The PMO or command must close all CAT I findings and close or mitigate all CAT II findings; mitigations must be approved by a fully qualified Validator.

- Existing C&A package diagrams, system/network hardware/software lists (including the DADMS number) and Ports, Protocols, and Services (PPS) must be updated.

The command or PMO deploying the eFP software and hardware must ensure the hardware and software remains STIG and IAVM compliant and supports the protection of Personally Identifiable Information (PII) throughout its life cycle.

Instructions for submitting fingerprints to OPM will be provided in separate guidance.

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
PEO IWS
PEO JSF

Subj: DEPARTMENT OF THE NAVY (DON) POLICY FOR APPROVING ELECTRONIC
FINGERPRINT (EFP) SOFTWARE AND HARDWARE FOR USE ON DON
NETWORKS

Distribution: (continued)

PEO LS

PEOLCS

PEO Ships

PEO Space

PEO Subs

DASN (C41 & Space)

COMPACFLT

COMUSFLTFORCOM

COMUSNAVEUR/USNAVAF

CNIC

USNA

NAVWARCOL

NAVPGSCOL

COMUSNA VCENT

COMFLTCYBERCOM

COMNAVAIRSYSCOM

COMNAVSEASYSYSCOM

COMNAVSUPSYSCOM

COMUSNAVSO

COMNAVFACENGCOM

COMNAVSPECWARCOM

COMSPAWARSYSCOM

DIRSSP

BUPERS

COMNAVDIST

ONI

FLDSUPPACT

COMOPTEVFOR

NAVIOCOM

COMMARCORSYSCOM

MARFORCYBER