



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

15 June 2011

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (RESEARCH,  
DEVELOPMENT AND ACQUISITION)  
ASSISTANT SECRETARY OF THE NAVY (ENERGY,  
INSTALLATIONS AND ENVIRONMENT)  
DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION  
OFFICER (NAVY)  
DEPARTMENT OF THE NAVY DEPUTY CHIEF INFORMATION  
OFFICER (MARINE CORPS)  
DEPARTMENT OF THE NAVY/ASSISTANT FOR  
ADMINISTRATION

Subj: DEPARTMENT OF THE NAVY (DON) SECURE HASH ALGORITHM MIGRATION  
GUIDANCE

- Ref: (a) FIPS PUB 201-1, Change Notice 1, Federal Information Processing Standards  
Publication, Personal Identity Verification (PIV) of Federal Employees and  
Contractors, March 2006  
(b) NIST Special Publication 800-78-3, Cryptographic Algorithms and Key Sizes for  
Personal Identity Verification, December 2010  
(c) NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning  
the Use of Cryptographic Algorithms and Key Lengths, January 2011  
(d) DoD CIO Memo, DoD's Migration to Use of Stronger Cryptographic Algorithms, of  
14 October 2010.

On 01 January 2011, the Federal Government, excluding Department of Defense (DoD), began use of Federal Personal Identity Verification (PIV) credentials, signed using the Secure Hash Algorithm (SHA)-256. The Federal Government initiated this action to strengthen the cryptographic hash standard supporting authentication practices prescribed by references (a), (b) and (c). As a result of DoD not transitioning to the use of SHA-256 signed Common Access Card (CAC) credentials, DoD systems, applications and websites that previously could authenticate Federal PIV card credentials now have interoperability issues.

To restore credential interoperability and enhance cryptographic security standards, the DoD will migrate from the use of SHA-1 to SHA-256. The scope of the DoD migration will include all unclassified and classified systems and applications using SHAs to support DoD Public Key Infrastructure (PKI) authentication, digital signature generation and email encryption/decryption. To align with Federal PIV and industry partner PIV-Interoperability migration efforts, DoD is developing migration planning guidance directing DoD PKI and Real-Time Automated Personnel Identification System infrastructure upgrades to support the DoD issuance of SHA-256 compliant CACs starting 01 January 2014. When the DoD SHA-256

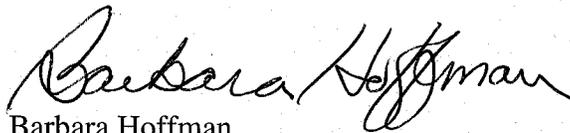
Subj: DEPARTMENT OF THE NAVY (DON) SECURE HASH ALGORITHM MIGRATION GUIDANCE

migration planning guidance is available, I will evaluate the effect of the DoD guidance on this memorandum, and provide further guidance as necessary.

In reference (d), the DoD CIO directs Component CIOs to develop and implement appropriate system and application portfolio (i.e., network, application, web portal and device) fixes to meet 31 December 2013 migration cryptographic requirements. To best align Department of the Navy (DON) SHA-256 migration plans with pending DoD planning guidance, DON Components will transition all affected systems, applications and websites to support SHA-256 no later than 01 April 2014. I recognize that operational deployment schedules may adversely affect a 01 April 2014 migration timeline for some impacted IT programs. However, there is a need to synchronize DON efforts with broader DoD PKI implementation activities to retain interoperability with DoD and other Federal agencies and industry partners.

I am establishing a DON multi-disciplinary SHA-256 migration Integrated Product Team (IPT), to support DON migration coordination and provide information that supports planning. The IPT will include representatives from the Offices of the DON Chief Information Officer (CIO), DON Deputy CIOs (Navy and Marine Corps), Assistant Secretary of the Navy for Energy, Installation and Environment, Deputy Assistant Secretary of the Navy (C4I and Space), and DON Administrative Assistant, to facilitate DON SHA-256 migration efforts in accordance with reference (d). While the offices identified here will be the organizational focal points responsible for DON-level coordination, other subject matter experts and stakeholders may be asked to provide expertise. The IPT will work closely with existing DoD-level SHA-256 migration efforts to share information, coordinate solution interoperability, and prevent unnecessary duplication of work.

The DON CIO points of contact for this are Mr. Roddy Staten, Roddy.staten@navy.mil, 703-695-2921, and Mr. James Mauck, James.Mauck.ctr@navy.mil, 703-697-0001.



Barbara Hoffman  
Department of the Navy  
Chief Information Officer (Acting)

Copy to:

CNO (DNS, N091, N093, N095, N097, N1, N2/N6, N3/5, N4, N8)

CMC (ACMC, ARI, M&RA, I, I&L, PP&O, C4, P&R)

COMFLTCYBERCOM

COMUSFLTFORCOM

COMUSNAVEUR USNAVAF

COMPACFLT

USNA

COMUSNAVCENT

COMNAVRESFORCOM

Subj: DEPARTMENT OF THE NAVY (DON) SECURE HASH ALGORITHM MIGRATION  
GUIDANCE

Copy to: (continued)

COMNAVAIRSYSCOM

BUMED

NETC

COMNAVSEASYSYSCOM

FLDSUPPACT

COMNAVSUPSYSCOM

DIRSSP

CNIC

COMNAVLEGSVCCOM

NAVPGSCOL

COMNAVFACENGCOM

COMNAVSAFECEN

BUPERS

NAVWARCOL

COMUSNAVSO

ONI

COMNAVSPECWARCOM

COMSPAWARSYSCOM

COMNAVDIST

NAVHISTHERITAGECOM

NAVY BAND

COMOPTEVFOR

PM NMCI ARLINGTON VA