



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JAN 03 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD SHA-256 Cryptographic & Hash Algorithm Transition Guidance

HSPD-12 established a Government-wide standard for secure and reliable forms of identification. FIPS Pub 201-1, NIST SP800-131A and NIST SP800-73-3 specify the architecture and technical requirements for a common identification standard for Federal employees and contractors. As discussed in DoD CIO Memorandum, "*DoD's Migration to Use of Stronger Cryptographic Algorithms*," dated October 14, 2010, in order for DoD to issue and utilize SHA-256 cards in accordance with federal requirements, it must first transition its IT infrastructure to support use of the SHA-256 algorithm.

The federal requirements have created concerns for DoD given the realities of a budget-constrained environment. Transitioning by the federal deadlines will divert a substantial portion of the DoD IT budget to this task, and has the potential to disrupt internal DoD operations if done incorrectly. Yet, a delayed transition could have a potentially disruptive impact on interoperability with those federal and industry partners who have or are transitioning toward using the SHA-256 algorithm in the near future.

Given these realities, DoD's goal is to move towards compliance with the federal guidance through planned and budgeted technology refreshes and upgrades. Accordingly, the DoD CIO directs all DoD Component CIO's to take the following actions:

- Effective immediately, all COTS software purchased as part of scheduled and budgeted technology refreshes and upgrades (on both NIPRNET and SIPRNET) must be SHA-256 compliant (i.e., will have embedded support for use of the SHA-256 algorithm in the purchased software).

- All DoD information systems that have been upgraded or are upgrading to support SHA-256 must continue to maintain backwards compatibility with DoD's current SHA-1 credentials.
- If a Component cannot ascertain from the vendor whether a product is SHA-256 compatible, they should contact their SHA-256 Coordination Cell Component representative. Additional information can be found in Attachment A of this memo, and/or by contacting SHA256_transition@osd.mil.
- If a Component system regularly interacts with federal or industry partners as part of its mission, then the system owner is encouraged to carefully consider the readiness of those partners to support SHA-256 based functions when developing their upgrade plans, so as to limit interoperability difficulties.
- Components will conduct a thorough review of their existing budget projections for planned IT infrastructure refreshes and upgrades, and provide the requested information in Attachment B. Based on these budget projections, they will also provide an estimated date of 100% completion to supporting SHA-256. This assessment is due 30 days after the issuance of this memo, and will be sent to SHA256_transition@osd.mil.

For additional information about this memorandum, my point of contact is Mr. Tim Fong at email: timothy.fong@osd.mil, (703) 614-1991.



Teresa M. Fakai

Attachments:
As stated

Attachment A: References

In cooperation with DMDC, DISA PKE and the DoD Components, the DoD CIO has gathered a significant amount of data on SHA-256 product support. This information should help Components conduct the requested assessments.

PKI-Based Capabilities

There are four PKI-based capabilities currently used by all Component organizations: Crypto-Logon to the NIPRNET, Reading and exchanging E-mail, Digitally signing and/or encrypting electronic data, and PKI-based web server authentication. Each capability must be able to use the SHA-256 signed certificates. The following table aligns the four PKI-based capabilities with some of the more commonly-used products and applications that support them:

<u>PKI Capability</u>	<u>Product Type</u>	<u>Product/Application Supporting SHA-256</u>
Crypto-Logon	Domain Controller software	MS Server 2003 w/ hotfix MS Server 2008
Reading digitally signed E-mail	E-mail software	MS Outlook 2003, 2007, or 2010
Digitally-Signing/encrypting data	Digital-signing software	
PKI-based client-side authentication to web-based systems	Server OS	MS Server 2003 w/ hotfix MS Server 2008 Apache 2.2.3-31-Mod_ssl 2.2.3-31 Apache 2.2.3-31-Mod_nss 2.2.3-31
	Internet Browser	Internet Explorer 7 or 8 Firefox 3.0.11, 3.6.6, or 3.6.8
All Capabilities	Workstation OS	MS Vista SP2 MS Windows 7
	Card Reader Middleware	Active Client 6.2.0.50
	Certificate Validation	Tumbleweed DV 4.9.2.172

Cryptographic Modules

NIST has collected technical information on a large number of cryptographic modules, including SHA-256 compatibility info.

<u>NIST Policy</u>	<u>Link</u>	<u>Notes</u>
FIPS 140	http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm	The "Cryptographic module" column has links to the Security Policy for each product, and many of these contain SHA-256 compatibility information. Also, see the "Level/Description" column for info on a few products.
FIPS 140	http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm	This FIPS 140 site focuses specifically on the Secure Hash Algorithm.
FIPS 201	http://fips201ep.cio.gov/ap1.php	The last column of the table is "Support for SHA-256."

General Vendor Information

The following table provides some links where components can find more information on products they may need to upgrade:

<u>Vendor</u>	<u>Product</u>	<u>Links and Notes</u>
Microsoft	Server & Workstation OS, E-mail Support	http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx
Mozilla	Network Security Services Plug-in (NSS)	http://www.mozilla.org/projects/security/pki/nss/ ; http://www.mozilla.org/projects/security/pki/nss/nss-3.11/nss-3.11-algorithms.html
Oracle	Various relevant products	http://iase.disa.mil/pki-pke/sha256/index.html

Further information on SHA-256 product compatibility can be found in the FOUO SHA-256 snapshot. The snapshot is located on a PKI-protected webpage of the DISA IASE site <http://iase.disa.mil/pki-pke/sha256/index.html>, and will be updated periodically. As some of the information in the snapshot is proprietary, please do not share it outside DoD.

Attachment B: Assessment

Components will provide information on their planned and budgeted IT infrastructure refreshes and upgrades through FY 2017. Components will report percentages for the NIPRNet and SIPRNet separately. If the Component will not reach 100% for either the NIPRNet or SIPRNet by FY 2017, it will provide information for that network for all years until it reaches 100%.

Workstation SHA-256 compliance

% of NIPR and SIPR-connected workstations upgraded to SHA-256 compatible workstation O/S
(Percentage is calculated as: Number of NIPR-connected workstations running WIN7 or VISTA/Number of NIPR-connected workstations in Component)¹

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible workstation O/S by EOFY 2012

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible workstation O/S by EOFY 2013

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible workstation O/S by EOFY 2014

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible workstation O/S by EOFY 2015

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible workstation O/S by EOFY 2016

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible workstation O/S by EOFY 2017

Middleware SHA-256 compliance

% of NIPR-connected wkstns upgraded to SHA-256 compatible middleware
(Percentage is calculated as: Number of NIPR-connected workstations running Active Client 6.2.0.0.50 or newer release/Number of NIPR-connected workstations in Component)¹

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible middleware by EOFY 2012

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible middleware by EOFY 2013

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible middleware by EOFY 2014

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible middleware by EOFY 2015

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible middleware by EOFY 2016

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible middleware by EOFY 2017

¹ Suggestion: do not adjust denominator in percentage calculation for small yearly fluctuations in the total number of workstations managed by the Component

Certificate validation software with SHA-256 compliance

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W
(Percentage is calculated as: *Number of NIPR-connected workstations running Tumbleweed 4.9.2.172 or newer release/Number of NIPR-connected workstations in Component*)¹.

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W by EOFY 2012

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W by EOFY 2013

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W by EOFY 2014

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W by EOFY 2015

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W by EOFY 2016

% of NIPR and SIPR-connected wkstns upgraded to SHA-256 compatible validation S/W by EOFY 2017

SHA-256 compliance supporting Cryptographic logon to the NIPRNET

% of NIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S
(Percentage is calculated as: *Number of NIPR-Domain Controllers running on MS Server 2003(+hotfix) or WIN 2008 /Number of NIPR-Domain Controllers in Component*)²

% of NIPR and SIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S by EOFY 2012

% of NIPR and SIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S by EOFY 2013

% of NIPR and SIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S by EOFY 2014

% of NIPR and SIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S by EOFY 2015

% of NIPR and SIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S by EOFY 2016

% of NIPR and SIPR-Domain Controllers upgraded to SHA-256 compatible Server O/S by EOFY 2017

² Suggestion: do not adjust denominator in percentage calculation for small yearly fluctuations in the number of Domain Controllers managed in the Component

SHA-256 compliance supporting PKI-based client authentication to web server

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2012

(Percentage is calculated as: Number of NIPR-connected servers running web-based business or mission systems on MS Server 2003(+hotfix), WIN 2008 or Apache 2.2.3/Number of NIPR-connected web-servers in Component)³

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2012

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2013

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2014

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2015

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2016

% of NIPR and SIPR-servers upgraded to SHA-256 compatible Server O/S by EOFY 2017

SHA-256 compliance supporting reading digitally signed email

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client

(Percentage is calculated as: Number of NIPR-connected workstations running MS Outlook versions (2003/2007/2010) /Number of NIPR-connected workstations in Component)¹

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client by EOFY 2012

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client by EOFY 2013

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client by EOFY 2014

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client by EOFY 2015

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client by EOFY 2016

% of NIPR and SIPR Email client software upgraded to SHA-256 compatible email client by EOFY 2017

³ Suggestion: Do not adjust denominator in percentage calculation for small yearly fluctuations in the number of web servers managed in the Component. Estimate number of web-servers operated within DISA's DECC.