

Attention Disbursing Officers and Supply Officers

**NAVY CASH[®]
SOP CHANGE NOTICE
NAVSUP PUB 727**

**Navy Cash Fleet Support Groups
NAVSUP Fleet Logistics Centers
Norfolk
San Diego
Yokosuka**

Navy Cash SOP Change Notice 2013-008

16 August 2013

Subject: **MAINTAINING LAPTOP SECURITY PATCHES AND UPDATES**

Attention: Disbursing Officers/Supply Officers

1. Background. The Navy Cash Information Assurance (IA) team conducts regular security audits. They review system reports that list the security vulnerability patches that have been applied on all the Navy Cash servers, workstations, and laptops, they monitor remote-access sessions, and they conduct on-site security reviews and inspections on Navy Cash ships. One common finding is that anti-virus definitions and other security patches are not always up to date on Navy Cash servers, workstations, and laptops. Frequently, the problem is with the “spare” laptop, which is intended as a backup for the Navy Cash workstation in Disbursing. Navy Cash servers and workstations are generally connected to the ship’s network at all times. Laptops, on the other hand, may be kept in storage.

Disbursing Officers (DOs) must ensure any laptop in storage, e.g., the spare laptop or the Marine Disbursing laptop (on LHA/LHDs), is connected to the ship’s network and powered up at least once each week, preferably near the end of the week (Thursday), for at least 48 hours each time, to make certain the laptop stays up to date with security updates and other software patches. One recommendation is that the laptop be connected to the network every Friday and left on over the weekend. If there is no dedicated LAN drop for the laptop, DOs may need to disconnect the workstation to connect the laptop to the network. The laptop should be powered up and remain on the log-in screen. Updates will generally occur automatically, but some updates will require a reboot, so DOs must be proactive and verify that the reboot process was completed. With regular updates, the spare laptop will be ready if it is ever needed as a backup and will not spend the first few hours updating anti-virus definitions and other security and software patches.

2. Disbursing Officer Action. Upon receipt of this Navy Cash SOP Change Notice, DOs must take the necessary steps to ensure all Navy Cash laptops are connected to the ship’s network at least once each week so that security patches and updates can be applied automatically.

3. Official Change to Navy Cash SOP. This Navy Cash SOP Change Notice represents an official change to the Navy Cash SOP (NAVSUP PUB 727). Each DO shall retain a copy of this Navy Cash SOP Change Notice on file for inspection with the current version of the SOP.

4. List of Effective Navy Cash SOP Change Notices.

2012-001—Automatic EOD Now Mandatory *CANCELED*

2012-002—Required Navy Cash Documentation in Financial Returns *CANCELED*

2012-003 Residual Funds on Visitor Cards

Please route immediately to the Supply Officer and Disbursing Officer

- 2012-004 Transfer Member Profile and Unsuspend Account Using Disbursing Web Site
- 2012-005 Automated Transfer of Dormant Profiles
- 2012-006 Navy Cash Depot Shipping Address Change
- 2012-007 Navy Cash, Marine Cash, and Navy Cash Visitor Card Cardholder Agreement
- 2012-008 Staff, Air Wing, Squadron, and Generic Private Merchants Settle Only to Merchant Strip Account
- 2012-009 Bank/Credit Union Account Information on Cardholder Web Site
- 2012-010 Automated EOM Spreadsheet Alternative
- 2012-011 Court Orders and Levies and Subpoenas on Navy Cash Accounts
- ~~2013-001 Enrollment Forms Missing in Document Storage System Ashore CANCELED~~
- 2013-002 Updating Generic Private, Staff, Air Wing, and Squadron Merchant Linked Accounts at Turnover
- 2013-003 Use of Official Mail Manager Merchant Card Now Mandatory
- 2013-004 Update to Navy Cash Cardholder Web Site
- 2013-005 Enrollment Forms Missing in Document Storage System Ashore—Revised
- 2013-006 Distribution of Ship's Store Profits to MWR and Other Miscellaneous Payments — Revised Procedures
- 2013-007 DASR and Revision to the Navy Cash Documentation Required in Financial Returns
- 2013-008 Maintaining Laptop Security Patches and Updates

5. Points of Contact. If you have any questions, please contact:

Karl Larson at NAVSUP Headquarters
 Navy Cash Information Assurance Officer
 karl.larson1@navy.mil
 (717) 605-3506 DSN: 430-3506

Hugh Chin at NAVSUP FLC Norfolk
 hugh.chin@navy.mil
 (757) 443-1189 DSN: 646-1189

Andy Yager at NAVSUP FLC San Diego
 andrew.yager@navy.mil
 (619) 556-6493 DSN: 526-6493

Joel Ignacio at NAVSUP FLC Yokosuka
 joel.ignacio@fe.navy.mil
 +81 (46) 816-7324 DSN: (315) 243-7324

§§§§§

8.4.33 Installation Alerts: Installing IAVA and Other Software Patches
(in version 1.14 of the Navy Cash SOP associated with release v1.4.7)

8.4.37 Installation Alerts: Installing IAVA and Other Software Patches
(in version 1.13 of the Navy Cash SOP associated with release v1.4.6)

a. Information Assurance Vulnerability Management (IAVM) is an important step in maintaining the security posture of the Navy Cash system. To effectively safeguard the Navy Cash system against internal and external cyber threats, all known vulnerabilities must be patched effectively in a timely manner.

b. Installation alerts provide an automated mechanism for applying software updates to the Navy Cash system on the ship. These software updates include Information Assurance Vulnerability (IAV) patches to address applicable Information Assurance Vulnerability Alerts (IAVAs) and Bulletins (IAVBs), DMLs (data fixes) applied to the ship-side Navy Cash database, and application patches applied to the Navy Cash system.

(1) When IAV and Navy Cash application patches have been pulled to the ship as a part of the round-trip process, the “Installation Alert” pop-up window will appear the next time an authorized individual logs in to the Disbursing Application. The Installation Alert window notifies the Disbursing Officer to initiate the installation process by clicking on the “Install Now” or to delay the installation by clicking on the “Install Later” button.

(2) DML patches will generally be transmitted to the ship and applied automatically without any action required by the Disbursing Officer.

c. The Disbursing Officer must install IAV and Navy Cash application patches as soon as practicable. Ideally, patches should be installed after the end of the business day, when retail outlets have closed out for the day and retail operations are at a minimum.

(1) If updates have not occurred for a while, reboot the system to attempt to force the update to restart, as there may have been an issue with the update script.

(2) The status of each patch will be transmitted back to shore automatically via a log file as a part of the next ship-initiated round trip. These log files will show a summary of the activity that occurred during the installation of a patch.

(3) IAV patches in particular require Navy-wide compliance monitoring to ensure mitigation of security vulnerabilities. For each IAVA/B, the Navy Cash IA team ashore must report compliance to meet established deadlines using the Online Compliance Reporting System (OCRS) and Vulnerability Management System (VMS), which are used to document and track compliance status for all Navy assets.

d. Ensure Laptops Connected Once Each Week. The Disbursing Officer must ensure any laptop in storage, e.g., the spare laptop or the Marine Disbursing laptop (on LHA/LHDs), is connected to the ship’s network and powered up at least once each week, preferably near the end of the week (Thursday), for at least 48 hours each time, to make certain the laptop stays up to date with security and other software patches. One recommendation is that the laptop be connected to the network every Friday and left on over the weekend. If there is no dedicated LAN drop for the laptop, the Disbursing Officer may need to disconnect the workstation to connect the laptop to the network. The laptop should be powered up and remain on the log-in screen. Updates will generally occur automatically, but some updates will require a reboot, so the Disbursing Officer must be proactive and verify that the reboot process was completed. With regular updates, the spare laptop will be ready if it is ever needed as a backup and will not spend the first few hours updating anti-virus definitions and other security and software patches.

e. Verify Update Process Completed

(1) IAV and Other Software Patches. To better maintain IAVM compliance of Navy Cash servers, workstations, and laptops on board ship, Navy Cash has implemented Windows Server Update Services (WSUS) (for software release 1.4.6 build 3 and 3a) and BMC Patch Manager (for software release 1.4.7 build 0 and later) to enable IAV and other software patches, such as bug fixes and new functionality, to be provided remotely and applied automatically.

(a) After a patch or update has been reviewed, tested, and approved by the Navy Cash Technical Support group (NCTS) at JPMorgan Chase (JPMC), it is placed on a server and waits for the Navy Cash computers on each ship to check-in with the server. The server lets the computer on the ship know which patches and updates have been approved but not yet installed.

(b) When a Navy Cash computer downloads a software patch or update, the computer determines if the item can be installed immediately without adversely affecting operations, i.e., the computer will not require a reboot. Otherwise, the computer queues the patch or update for installation at a scheduled timeslot.

((1)) For Server Node-1, installation begins each Friday at 0300 GMT.

((2)) For Server Node-2, installation begins each Saturday at 0300 GMT.

((3)) For workstations and laptops, installation begins each Friday at 1000 GMT.

(2) Anti-Virus Definitions. Symantec's anti-virus LiveUpdate solution on the Navy Cash servers, workstations, and laptops has been configured to automatically retrieve virus definitions on a daily basis (at 1000 GMT) directly from Symantec (software release 1.4.6 build 3a and later).

(a) When LiveUpdate determines that a newer file is available, it initiates a download directly from Symantec. Once the download is successfully received, Symantec's anti-virus application processes the download and implements the new settings.

(b) To verify the update process was completed and the virus definitions file version is up to date, the Disbursing Officer must check the main Symantec Antivirus (or Endpoint Protection) window to confirm that the file date is not more than one day older than the present date or that the "Protection definitions are current" link is displayed.

(c) If the automated update function does not appear to be running, the updates can be applied manually by clicking on the "LiveUpdate" button or link. If the date is older than seven days, contact the Navy Cash Central Support Unit (CSU) at 1-866-662-8922 or navycashcenter@ezpaymt.com and request assistance.

f. IT-21 Security Practices. The disbursing office should follow IT-21 security practices, e.g., auditing event logs, physical security, etc., in addition to any Navy Cash security requirements (see primarily paragraphs 8.2, General; 8.3, Navy Cash Custodial Responsibilities; and 8.4.32, Access Editor–Access Control for Disbursing Application).

(1) Retina Vulnerability Scanner. The eEye Retina Vulnerability Scanner is an enterprise vulnerability scanning tool approved for use by the Department of Defense. Ships' ITs use Retina to remotely scan all computer networks and assets on the ship to help track IAVM compliance. Navy Cash is an approved afloat system, and the Retina scanner is approved for use in scanning the Navy Cash system.

(2) Occasionally, a scan conducted on the ship may reveal a security vulnerability on the Navy Cash system that requires a patch or update. As described above in paragraph e.(1), the Navy Cash Program Office at NAVSUP manages all vulnerabilities and patches with the assistance of NCTS at JPMC and Engility. Security vulnerability patches and updates are reviewed, tested, and approved in the Navy Cash lab

to ensure that any patch or update applied will not damage the operation of the Navy Cash system on the ship. Approved patches and updates are provided remotely and applied automatically. At no time should a patch be applied to an afloat Navy Cash system without the direct assistance of NCTS at JPMC or Engility.

(3) Any patch or update applied to the Navy Cash system without NCTS or Engility assistance is considered unauthorized and may be subject to investigation. The Navy Cash Program Office understands that Navy organizations inspecting afloat systems may insist that patches be applied immediately, but doing so would represent a departure of the Navy Cash system on the ship from the approved baseline of its ODAA type accreditation.

(4) If the ship's ITs or other personnel have questions regarding this matter or a Disbursing Officer is notified by the ship's ITs or other personnel that a patch or other software (HBSS, etc.) must be installed on the Navy Cash system, please contact the NAVSUP Navy Cash Program Office Information Assurance Officer (IAO) (phone: (717) 917-3506) or the CSU to coordinate the technical details, since any new, untested software install like this may adversely affect Navy Cash operations on the ship if it is configured incorrectly in any way.