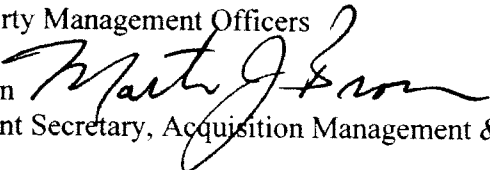




LOGISTICS POLICY MEMORANDUM 2009 - 01

JAN 12 2009

To: All HHS Property Management Officers

From: Martin J. Brown 
Deputy Assistant Secretary, Acquisition Management & Policy (ASAM/OAMP)

Subject: Sensitive Items Policy for Personal Property and Equipment

Effective: January 1, 2009

This memorandum revises the current policy regarding the treatment of Sensitive Items to require the inclusion of all Personal Property and Equipment (PP&E) in the Property Management Information System (PMIS) if the item meets any of the criteria set forth in the attached policy statement (see Attachment 1). This policy does not apply to real property or to contractor-held property, on-site or off-site (*see* revised Federal Acquisition Regulations Part 45) or to PP&E leased by a contractor for use by HHS. This policy will be incorporated in the HHS Logistics Management Manual as part of the next revision cycle in 2009.

To assist in implementing the revised policy, we have included a revised sensitive equipment list as guidance. If an OPDIV/STAFFDIV believes a particular item of PP&E should be tracked as a sensitive item, the OPDIV Property Management Officer (PMO) must validate that the item is critical to the mission, in accordance with the procedures stated in the policy, prior to inclusion in the PMIS. All OPDIVs and STAFFDIVs should review and resubmit their OPDIV-specific lists to OAMP/DLP by March 31, 2009 for approval consideration.

Questions concerning this policy should be directed to the HHS Director of Logistics Policy, Mr. James Begis, at (202) 205-1239 or james.begis@hhhs.gov.

Attachment:

cc: HHS OPDIV/STAFFDIV – Agency Heads

Sensitive Items

A Sensitive Item is defined at 41 CFR § 102-35.20¹ as Personal Property & Equipment* that “includes all items, **regardless of value**, that require special control and accountability due to unusual rates of loss, theft or misuse, or due to national security or export control considerations. Such property includes **weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment**. These classifications do not preclude agencies from specifying additional personal property classifications to effectively manage their programs.” (emphasis added)

The following is a example list of Sensitive Items:

Category	Minimum Acquisition Threshold	Examples include:
Multi-functional Office Equipment**	\$300.00	Computer and video projectors, fax, copiers, scanners, & digital senders.
Computers**	No minimum acquisition cost.	Includes PCs, servers, laptops, & micro-mini laptops.
Personal Digital Assistant with PC Connectivity**	No minimum acquisition cost.	Palm Pilot, Palm M505, Blackberry's & Handspring.
Portable Hard Drives**	No minimum acquisition cost	Does not include smart cards, USB memory sticks or other devices classified as “media”.
Power Tools	\$300.00	Includes stand alone items such as Portable compressors, generators, or table saws.
Video Recorders/players	\$300.00	Video (VCR), tape, dictation machines, digital compact audio disc (CD), digital video disc (DVD), & audio tape.
Portable Instrumentation	\$300.00	Voltmeters, O-scopes, & Watt Meters
Hazardous Materials***	No minimum acquisition cost	Radioactive, chemical, nuclear materials & Reagents. (See 40 CFR part 261)
Still Cameras	\$300.00	Digital, Laparoscopic, & , X-ray Identification
Video Cameras	\$300.00	Does not include surveillance equipment.
Weapons	No minimum acquisition cost	Firearms, knives, etc.
Precious Metals (or equipment made of same)****	No minimum acquisition cost	Gold, Silver, Platinum, & Silver.

¹ See http://edocket.access.gpo.gov/cfr_2008/julqtr/41cfr102-35.20.htm.

* The PMIS and this policy do not apply to real property acquired by HHS, its OPDIVs or STAFFDIVs. Nor does it apply to contractor held property, on-site or off-site (see revised Federal Acquisition Regulations Part 45) or to PP&E leased by a contractor for use by HHS.

** *With respect to the contents of these items, see generally -*
<http://intranet.hhs.gov/infosec/guidance.html> *and specifically -*
http://intranet.hhs.gov/infosec/docs/policies_guides/HM/Havekost_Memorandum_ISP-2007-005.htm and
http://intranet.hhs.gov/infosec/docs/guidance/hhs_standard_2007.pdf (footnote 2).

****See also* Logistics Management Manual - §103-42.003 HHS HAZARDOUS MATERIAL MANAGEMENT.

****This is not intended to include items that contain small or trace amounts of precious metals, e.g., printed circuit boards.

HHS Standard 2009-0001.001S
January 30, 2009

To implement Federal Acquisition Regulation (FAR) 39.101(d) regarding Common Security Configurations, and Department of Health and Human Services (HHS) information security requirements, the following standard language shall be incorporated in solicitations and new contracts for the operation or acquisition of information technology systems. This document supersedes HHS Standard 2008-0004.001S, *HHS-OCIO Standard for Security Configurations Language in HHS Contracts* (dated September 11, 2008), and is effective immediately.¹ An approved *HHS Department Information Security Policy/Standard Waiver*² is required to deviate from the technical standard set forth below.

1. Contractor computers containing HHS data shall be configured with the applicable Federal Desktop Core Configuration (FDCC) (<http://nvd.nist.gov/fdcc/index.cfm>),³ and shall have and maintain the latest operating system patch level and anti-virus software level.
2. The Contractor shall apply approved security configurations to information technology that is used to process information on behalf of the Department, its Operating Divisions (OPDIVs) and Staff Divisions (STAFFDIVs).

Such approved security configurations shall be identified jointly by the OPDIV/STAFFDIV Contracting Officer's Technical Representative (COTR) and Chief Information Security Officer (CISO). Approved security configurations include, but are not limited to, those published by the Department,⁴ by the OPDIV/STAFFDIV, and by the National Institute of Standards and Technology (NIST) at <http://checklist.nist.gov>. OPDIVs/STAFFDIVs may have security configurations that are more stringent than the minimum baseline set by the Department or NIST. When incorporating such security configuration requirements in solicitations and contracts, the OPDIV CISO shall be consulted to determine the appropriate configuration reference for a particular system or services acquisition.

3. The Contractor shall ensure applications operated on behalf of the Department or OPDIV/STAFFDIV are fully functional and operate correctly on systems configured in accordance with the above configuration requirements. The Contractor shall use Security Content Automation Protocol (SCAP)-validated tools with FDCC Scanner capability to ensure its products operate correctly with FDCC configurations and do not alter FDCC settings.⁵ The Contractor shall test applicable product versions with all relevant and current updates and patches installed. The contractor shall ensure currently supported versions of information technology (IT) products meet the latest FDCC major version and subsequent major versions.⁶
4. The Contractor shall ensure applications designed for end users run in the standard user context without requiring elevated administrative privileges.
5. The Contractor shall ensure hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements specified above
6. Federal Information Processing Standard 201 (FIPS-201)⁷ compliant, Homeland Security Presidential Directive 12 (HSPD-12) card readers shall: (a) be included with the purchase of servers, desktops, and laptops; and (b) comply with FAR Subpart 4.13, *Personal Identity Verification*.
7. The Contractor shall ensure all its subcontractors which perform work under this contract (at all tiers) comply with the above requirements.

HHS Standard 2009-0001.001S
January 30, 2009

APPROVED BY & EFFECTIVE ON:

_____/s/
Michael W. Carleton
HHS Chief Information Officer and
Deputy Assistant Secretary for Information Technology

January 30, 2009
Date

_____/s/
Martin J. Brown
HHS Senior Procurement Executive and
Deputy Assistant Secretary
for Acquisition Management and Policy

January 30, 2009
Date

¹ This requirement will be incorporated into the HHS Acquisition Regulation and the HHS Acquisition Plan.

² The *HHS Departmental Information Security Policy/Standard Waiver* form and process is available at http://intranet.hhs.gov/infosec/policies_memos.html.

³ FDCC is applicable to all computing systems using Windows XP™ and Windows Vista™, including desktops and laptops—regardless of function—but not including servers. The Department has developed an HHS version of FDCC (henceforth HHS FDCC) for Windows XP™ and Vista™ to accommodate business and operational needs in the HHS environment. These settings are available at <http://intranet.hhs.gov/infosec/guidance.html>. When there is a compelling business or operational need to deviate from the FDCC, Operating Divisions (OPDIVs) and Staff Divisions (STAFFDIVs) may use the HHS FDCC settings instead of the government-wide FDCC settings.

⁴ See *HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications* (as amended) at <http://intranet.hhs.gov/infosec/guidance.html>.

⁵ See <http://nvd.nist.gov/validation.cfm>, as required by the Office of Management and Budget (OMB) Memorandum (M) 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, released August 11, 2008.

⁶ This meets the self-assertion requirement under OMB M-08-22. Future FDCC changes having minimal security impact may be released as minor versions to FDCC. Self-assertion is not required for minor releases.

⁷ <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

HHS Standard 2009-0002.001S

January 30, 2009

The Department of Health and Human Services (HHS) requires incorporation of the following standard language in solicitations and new contracts that either purchase or require the use of desktop or laptop computers, mobile devices, or portable media to store or process HHS sensitive information that is categorized as Moderate or High under Federal Information Processing Standard 199 (FIPS 199).¹ An approved *HHS Department Information Security Policy/Standard Waiver*² is required to deviate from these technical standards. This standard is effective immediately.³

1. The Contractor shall use FIPS 140-2 (as amended) compliant encryption⁴ to protect all instances of HHS sensitive information⁵ during storage and transmission.
2. The Contractor shall verify that the selected encryption product has been validated under the Cryptographic Module Validation Program (<http://csrc.nist.gov/cryptval/>) to confirm compliance with FIPS 140-2 (as amended). The Contractor shall provide a written copy of the validation documentation to both the Contracting Officer and the Contracting Officer's Technical Representative (COTR).
3. The Contractor shall use the Key Management Key on the HHS personal identification verification (PIV) card; or alternatively, the Contractor shall establish and use a key recovery mechanism to ensure the ability for authorized personnel to decrypt and recover all encrypted information.⁶
4. The Contractor shall securely generate and manage encryption keys to prevent unauthorized decryption of information, in accordance with FIPS 140-2 (as amended).
5. The Contractor shall: ensure that this standard is incorporated into the Contractor's property management/control system; or establish a procedure to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive HHS information.
6. The Contractor shall ensure that all of its employees, subcontractors (at all tiers), and employees of each subcontractor, who perform work under this contract/subcontract, comply with the above requirements.

APPROVED BY & EFFECTIVE ON:

_____/s/_____
Michael W. Carleton
HHS Chief Information Officer and
Deputy Assistant Secretary for Information Technology

January 30, 2009
Date

_____/s/_____
Martin J. Brown
HHS Senior Procurement Executive and
Deputy Assistant Secretary for Acquisition Management and Policy

January 30, 2009
Date

HHS Standard 2009-0002.001S
January 30, 2009

¹ FIPS-199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.

² The HHS Departmental Information Security Policy/Standard Waiver form and process is available at http://intranet.hhs.gov/infosec/policies_memos.html.

³ This requirement will be incorporated into the HHS Acquisition Regulation and the HHS Acquisition Plan.

⁴ The Office of Management and Budget (OMB) Memorandum (M) 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (released May 22, 2007) requires the use of FIPS 140-2, Security Requirements for Cryptographic Module, compliant encryption technologies on laptop computers and all other mobile computers and devices containing sensitive information. The HHS memorandum Mandatory Protection of Sensitive Information on Computers, Mobile Devices, and Portable Media (henceforth called the Protection of Sensitive Information Memo), signed by the HHS Chief of Staff on May 19, 2008, directs expansion of the current HHS Encryption Standard for Mobile Devices and Portable Media to “all government and non-government-furnished desktops used on behalf of the government that store sensitive information.”

⁵ For the purposes of this contract, information is considered sensitive if the FIPS 199 Confidentiality or Integrity security objective is rated Moderate or High by the OPDIV Chief Information Security Officer (CISO) or HHS Chief Information Security Officer (CISO), as appropriate.

⁶ Key recovery is required by OMB Guidance to Federal Agencies on Data Availability and Encryption, November 26, 2001, <http://csrc.nist.gov/policies/ombencryption-guidance.pdf>. Authorized personnel to decrypt and recover all encrypted information shall be identified by contract.