

National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546-0001



OCT 17 2005

Reply to Attn of: **Office of the Chief Information Officer**

TO: Distribution

FROM: Chief Information Officer (Acting)

SUBJECT: Meeting OMB Memoranda M-06-015 "Safeguarding Personally Identifiable Information;" M-06-016 "Protection of Sensitive Agency Information," and M-06-019 "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"

The inadvertent disclosure of sensitive data at several Federal Agencies has prompted OMB to issue three memoranda targeting the protection of this critical data. The memoranda are far reaching and address the protection of sensitive but unclassified (SBU) information, including privacy data. Particular attention is warranted for privacy data, given the Government's special responsibility to protect its citizenry.

This memorandum addresses the protection of SBU information that must be protected regardless of its location, especially when it resides on mobile computing devices that are often used in environments with limited or no physical security. An addendum to this memorandum prioritizes actions and provides milestones necessary to effectively and expeditiously safeguard this sensitive data.

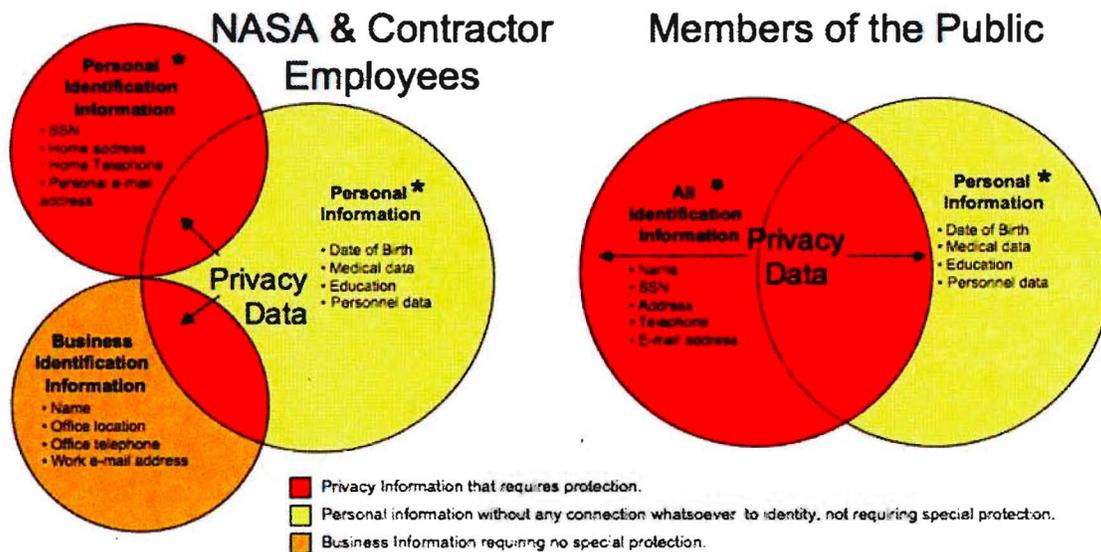
NASA's policy document, NASA Security Program Procedural Requirements (NPR) 1600.1, defines SBU information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled, but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

Privacy data is a subset of SBU data. The entire realm of information gathered and/or maintained by the Agency that is unique to specific individuals may be thought of as privacy data. This information is often referred to as either Personally Identifiable Information (PII) or Information in Identifiable Form (IIF) in various statutes and OMB memoranda. For the purposes of this memorandum, the two terms are interchangeable as shown in Figure 1. The figure differentiates privacy data that must be protected because of its association with one's identity (red shading) and data which does not require protection because it is completely unassociated with identity (e.g., abstracted or statistical data).

It is essential to understand that NASA may only collect and maintain information relating to employees, contractors, or other individuals when it is necessary to carry out a purpose of the Agency that is authorized by statute or an Executive order of the President of the United States.

NASA has made substantial progress in protecting this sensitive data. However, the Agency continues to review its processes and policies surrounding privacy data and is finalizing a NASA Procedural Requirement specifically for privacy data. Further, NASA has internalized Federal requirements in the Federal Information Security Management Act, adopting all requirements set forth by the National Institute of Standards and Technology (NIST). These requirements cover the entire IT security lifecycle, providing a risk management-based approach that safeguards NASA's systems and information in accordance with the sensitivity of the data.

Privacy Data Requiring Protection (Physical and Electronic)



Personally Identifiable Information (PII) - information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Information in identifiable form (IIF) - is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

*Lists are not comprehensive. Direct any questions of whether specific information should be regarded as privacy information to Center Chief Counsel.

Figure 1

Table 1 provides a list of OMB requirements that have been satisfied to date. However, much work lies ahead in safeguarding NASA's data. Table 2 (enclosed) provides a phased list of actions the Agency will undertake in order to meet information protection requirements. All NASA Centers and Mission Directorates must comply with these actions, as indicated.

Any questions regarding this memorandum can be sent to Michael Castagna (michael.j.castagna@nasa.gov) or Patti Stockman (patti.stockman@nasa.gov).

A handwritten signature in black ink, appearing to read 'John W. McManus', with a long horizontal flourish extending to the right.

John W. McManus

Enclosure

Completed and Open Actions Required to Meet the Requirements of the OMB Memoranda

Table 1 Completed Actions

#	OMB Requirement	Actionee	NASA: Phase I Rqt	Phase I Due Date	NASA: Phase II Rqt	Phase II Due Date
1	Remind employees of special responsibility to protect privacy data	OCIO	Deputy Administrator email reminding employees of special responsibility to protect privacy data	Completed	NA	NA
2	Use OMB checklist against all IT systems that contain privacy data	All Centers	Use OMB checklist against all IT systems that contain privacy data	Completed	NA	NA
3	Include training on privacy data in the IT Security and Awareness Training	OCIO	Include training on privacy data in the IT Security and Awareness Training	Completed	NA	NA
4	Review of privacy policies and processes (e.g., Checklist provided in M-06-16) on removal of privacy data beyond agency premises or control.	OCIO	Produce report on review with FY06 FISMA report	Completed	NA	NA
5	Require report of all incidents, suspected or confirmed, involving privacy data, in physical or electronic form within one hour.	All Centers	Report all incidents, suspected or confirmed, involving privacy data, in physical or electronic form within one hour to NASIRC.	Completed	NA	NA

Table 2: Open Actions

OMB Requirement	Actione e	NASA: Phase I Rqt	Phase I Due Date	NASA: Phase II Rqt	Phase II Due Date
Develop comprehensive privacy policy	OCIO	Finalize NPR 1382 linking privacy and IT security	1 Dec 06		
Encrypt all data on mobile computers/devices which carry agency data	All Centers and Mission Director ates	Allow for the encryption of SBU data on Windows and Apple laptops with Entrust or native encryption in Microsoft and Apple Operating Systems. Prioritize effort to address systems with highest likelihood of containing PII.	1 Apr 07	Allow for encryption of SBU data on non-Microsoft/Apple laptops and mobile devices (i.e., PDA), external storage devices (e.g., thumb drives) and/or apply requisite compensating controls.	1 Dec 07
	All Centers and Mission Director ates	Allow for the encryption of SBU data on Microsoft/Apple desktops with Entrust or native encryption in Microsoft and Apple Operating Systems.	1 June 07	Allow for the encryption of SBU data on non-Microsoft/Apple desktops with Entrust or native encryption in Microsoft and Apple Operating Systems.	1 Feb 08
	Desktop Standar ds	Investigate encryption of all SBU data on servers and databases.	1 June 08	Encrypt of all SBU data on servers and databases.	1 June 09
	Desktop Standar ds	Investigate encryption options for user data on mobile devices and/or the use of compensating controls	1 Jan 07	NA	NA
	OSPP	Prepare letter providing guidance/requirements on required physical security for external storage devices.	1 Jan 07	NA	NA
Allow remote access only with two factor authentication where one of the factors is provided by a device separate from the computer gaining access	All Centers and Mission Director ates	Only allow remote access to Center via: -Use of existing two-factor authentication if available. For those applications not using two factor authentication ensure they are scheduled as a priority for the NASA HSPD-12 implementation. -Where two factor is not possible, ensure a VPN service using SSL or IPsec.	1 Jun 07	High priority HSPD-12 implementation for High and Moderate systems with Privacy data	1 Dec 07

	Use a "time-out" function after 30 minutes of inactivity for remote access and mobile devices requiring user re-authentication	All Centers and Mission Directorates	For all remote access and mobile computing devices, implement remote access "time-out" after 30 minutes or less of inactivity.	1 Jan 07	NA	NA
	Log all computer-readable extracts from database holding sensitive information and verify each extract, including sensitive data, has been erased within 90 days or its use is still needed	Desktop Standards	Establish a process to log all computer-readable extracts of <u>privacy data</u> from databases holding sensitive information and verify each extract, including sensitive data, has been erased within 90 days or its use is still needed	1 Jul 07		

DISTRIBUTION:

Office of Security & Program Protection/Frank Martin

Center CIOs:

ARC/Sylvia Longchamps (Acting)

DFRC/Robert Binkley

GRC/Sasi Pillay

GSFC/Linda Cureton

HQS/Sandra Daniels-Gibson

JPL/James Rinaldi

JSC/Larry Sweet (Acting)

KSC/Michael Bolger

LaRC/Cathy Mangum

MSFC/Jonathan Pettus

SSC/Gay Irby

NSSC/Terry Jackson

Mission Directorate CIOs:

Aeronautics Research/Gary Cox (Acting)

Exploration Systems/Beverly Hamilton

Science/Joe Bredekamp

Space Operations/Chris Pino