POLICY FLASH 2006-46

POLICY FLASH 2006-46

DATE: August 16, 2006

TO: Procurement Directors

FROM: Office of Procurement and Assistance Policy, MA-61
Office of Procurement and Assistance Management

SUBJECT: Contractor Protection of Personally Identifiable Information (Pll)

SUMMARY: This Flash transmits infonnation provided by the Department's Chief Infonnation Office (CIO) regarding the DOE eontractor safeguard of government personally identifiable information, whether at or away from a government facility.

Background:

Recent breaches in the security of personal infonnation in the custody of federal government entities have resulted in the promulgation of guidance from the Office of Management and Budget (0MB) and the DOE CIO.

. What is the purpose of this initiative?

The purpose of this initiative is to apply protections offered by physical security controls when infonnation is removed or accessed from outside of a DOE agency location. As a result, recent 0MB and CIO guidance (listed below) concerning this subject is provided to ensure that all appropriate DOE contractors handling such infonnation are made aware of its requirements. This guidance is part of an aggressive DOE-wide implementation of the Cyber Security Revitalization Plan and is intended to implement the protection mechanisms of PH on all Federal information systems. To ensure consistent DOE-wide execution, 0MB has requested that the Inspector General (IG) review the implementation safeguards identified in its M-06-16 memorandum consistent with DOE cyber security compliance monitoring activities. Additionally, the CIO has provided a "working" list of

examples of what is and is not PII for the purpose of implementing cyber security guidance. Please find the following at http://cio.cloe.gov/Cybersec/index.html:

1. DOE CIO Memorandum dated July 25, 2006, "Transmittal of Recent 0MB Memoranda on Protecting Personally Identifiable Information" with attachments:

   a. 0MB Memorandum M-06-16 dated June 23, 2006, "Protection of Sensitive Agency Information"

   b. 0MB Memorandum M-06-19 dated July 12, 2006, "Reporting Incidents Involving Personally Identifiable Information and Incol'porating the Cost for Security in Agency Information Technology Investments"

2. DOE CIO Memorandum dated July 20, 2006, "Transmittal of Department of Energy Chief Information Officer Guidance-Protection of Personally Identifiable Information" with attached DOE CIO Guidance CS-38.

3. DOE Working Examples of Personally Identifiable Information dated August 9, 2006.

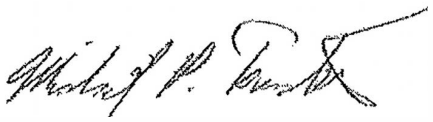
How will this affect work processes?

Contracting Officer's should inform and ensure contractors understand that under FAR 52.224-2, Privacy Act, protecting PII on laptops and removable storage media, whether in a government facility or accessed remotely, must be consistent with current DOE policy. Additional guidance may also be forthcoming,

Additional infonnation regarding DOE's PII Cyber Security initiative may be obtained from William Hunteman, OCIO. He can be reached on (202) 586-4775 or e-mail at Willia311.Hunjemat1@hq.doeJlliX·

This Flash may be viewed at h(!p://m:ofossionals.pr.doe.£ov.

Questions concerning this Policy Flash should be directed to Denise P. Wright at (202) 287-1340 or Denise.Wrigl!!@b,0oc.gov.



Michael P. Fischetti, Director
Office of Procurement and
Assistance Policy

Department of Energy
Washingt6n, DC 20686

July 20, 2006

MEMORANDUM FOR HEADS OF DEPARTME: EMENTS

FROM: THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER

SUBJECT: Transmittal of Department of Energy Chief lnfonnation Officer Guidance· Protection of Personally Identifiable Information

In keeping with the goals and processes outlined in the Cyber Security Program Revitalization Plan and to implement recent Office of Management and Budget (0MB) guidance, J am approving and issuing the auached Guidance, DOE CJO Guidance CS-38, Protection of Personally Identifiable Information.

This Guidance, which was developed by the Office of the Chief Information Officer (CIO) and reviewed by the Cyber Security Working Group, applies 0MB memorandum, M-06• I6, ***Protection of Sensitive Agency Information,*** and the sections of 0MB memorandum M-06-19, ***Reporting Incidents Involving Personally Jdelll!f/able Informal/on and Incorporating the Cost for Security in Agency Information Technology Jnvestme1lts,*** pertaining to the Protection of Personally Identifiable Information.

As we continue to issue Guidance as part of the aggressive implementation of the Cyber Security Revitalization Plan, l enlist your help to ensur that the criteria in this Guidance are promptly and adequately addressed within your organization. Key parts of this Guidance are to be fully implemented in early August 2006 according to the 0MB memorandum M-06· J6. Because of this, you and your staff should ensure that this Guidance is passed along quickly throughout your organization.

Please note that 0MB memorandum M-06-16 requests that the Inspector Ge.ner.ll review the implementation of the safeguards identified in that memorandum to ensure they are in place by August 9, 2006. In addition, implementation of this Guidance, Department• wide, will be included in the cyber security compliance monitoring activities carried out by the Office of the CIO, the Office of the Inspector General, and the Office of Security and Safety Performance Assurance.

Please contact Bill Hunteman, Associate CIO for Cyber Security, at 202-586-1090, for additional information.

Thank you for your personal attention to ensuring that the content of this new Guidance is integrated into your organization's cyber security program as soon as possible.

Attachment

DISTRIBUTION LIST

Secretary
Deputy Secretary
Under Secretary of Energy
    Assistant Soeretary for Energy Efficiency and Renewable Energy
    Assistant Secretary for Environmental Management
    Assistant Secretary for Fossil Energy
    Assistant Secretary for Nuclear Energy, Science and Technology
    Director, Office of Civilian Radioactive Waste Management
    Director, Office of Electricity Delivery and Energy Reliability
    Director, Office of Legacy Management
Under Secretary for Science
    Director, Office of Science
Under Secretary of Nuclear Security/Administrator National Nuclear Security Administration
Departmental Representative to the Defense Nuclear Facilities Safety Board
Assistant Secretary for Congressional and Intergovernmental Affairs
Assistant Secretary for Environment, Safety and Health
Assistant Secretary for Poiicy and International Affairs
Administrator, Energy Information Administration
Chief Financial Officer
Chief Human Capital Officer
Chief Information Officer
General Counsel
Inspector General
Director, Office of Economic Impact and Diversity
Director, Office of Hearings and Appeals
Director, Office of Human Capital Management
Director, Office of Management
Director, Office of Public Affairs
Director, Office of Security and Safety Performance Assurance
Power Marketing Administrations Liaison Office
Senior Intelligence Officer, Office of Intelligence and Counterintelligence

DOE <,1O Guidance CS-38

U.S. Department of Energy
Cyber Security Program

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION GUIDANCE

July 20, 2006

I. PURPOSE.

This Department o f Energy (DOE) Chieflnfonnalion Officer (CJO) Guidance applies the Office o f Management and Budget (0MB) memorandum, M-06-16, *Protection o f Sensitive Agency fl1formatio11,* and the sections o fOMB memorandum M-06-19, *Reporting Incidellls Involving Personally Identifiable Ieformation and Incorporaling the Costfo r Security in Agency I1iformation tecltnology Investments,* pertaining to the protection o f personally identifiable infonnation (Pl!).

The DOE CIO will review this Guidance annually and update it as necessary. Senior DOE Management and their operating units may provide feedback at any time for incorporation into the next scheduled update.

Attachment 2 contains the 0MB definition o fPll that should be used to implement this Guidance.

2. ;iCOPE.

This Guidance provides additional information for the protection o f PI! in all infonnation systems operated by the Department and its contactors.

3. CANCELLATIONS.

None.

4. APPLICABILITY.

a. primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Depar/menl o fEnergy Organizations to Which DOE CIO Guidance CS-38 is Applicable.*

Further, the DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chieflnfonnation Officer (CIO) (hereinafter referred to as Senior DOE Management) may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incoiporated into contracts.

b. Exclu!)ons. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director o f the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organiwtion o f the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.

c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE M 471.3· 1, *Manualf o r Identifying and Protecting Official Use Only Information,* and DOE M 471. 1•1, *Identification and Protection o f Unclassified Colllrolled Nuclear Infonnation Manual,* provide additional information for identifying unclassified information requiring protection.

d. National Security S n t ___ Senior DOE Management PCSPs are to address this Guidance for **all** DOE National Security systems. Executive Order **12829 (E.O.** 12829), which established the National Industrial Security Program; the requirements o f the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act o f 1954, which established Restricted Data information; DOE CIO Guidance CS-22, *Nat/011a/ Security Systems Controls Guidance;* and NIST SP 800-59, *Guideli11e11for Ide11tifyi11g an Information System as a National Security System,* provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective upon issuance. Except as noted below, DOE expects that Senior DOE Managen1ent shall address the criteria in this document within 30 days o f its effective date.

Tiiis implementation o f this guidance for the protection o f Pll on all Federal information systems must be completed by August 9, 2006, to be consistent with 0MB Memorandum M-06-16, *Protectio11 o f Sensitive Agency I,iformat/011,* dated June 23, 2006.

6. CRITERIA.

a. Program Cyber Security Plan. Senior DOE Management PCSPs are to direct operating units to develop, document, and implement PU policies and procedures consistent with criteria b. through e. immediately below.

b. Use o f Encryption

Implement the use ofFIPS 140-2 Level 1 or higher encryption to protect all Pl! on laptops and on removable media, such as CDROMs or thumb drives.

- All laptop computers used by Federal employees and contractors who support Federal systems that contain PJI should have an installed capability to encrypt all Pl!.
- All users oflhese laptops should be instructed to use this capability to protect all PH.

The following steps are to be followed to implement the criteria in this section:

- Identify all laptops that contain PI!.
- Remove PII from all laptops for which its presence is not essential.
- Install encryption software for all laptops that will continue to contain PH or that will contain PH in the future.
- Provide training to the user(s) on the use of the encryption software.
- Provide direction to the user(s) that the encryption software is to be used to protect all Pl! on the laptop.

It is recommended that the use of encryption protection be applied to laptops and all desktop computer systems as well, so as to provide increased protection against loss of portable devices and cyber attacks.

c. Two Factor Authenticatio!!

Use two-factor authentication for all individuals having remote access to PU other than their own.

d, Remote Access

Ensure that a time-out function is in place on all systems supporting remote access that requires re-authentication of remote users if there is a period of 30 minutes or longer of inactivity on their connection to the system.

e. Management of PH on Laptops and Removable Media

Establish and implement procedures throughout the organiwtion so that any files containing Pl! on laptops or removable media have been deleted, within 90 days, or that use of these files is still required.

Procedures are to include documentation of the regular use of these procedures for each laptop or removable media device that contains PH.

f. Reporting of incidents Involving PU

Ensure that all suspected or confirmed eyber security and physical security incidents involving Pll are reported to the DOE Cyber Incident Advisory Capability (CIAC) within 45 minutes of discovering the incident. CIAC is to report the incident to US-CERT within one hour of discovery of the incident.

When reporting incidents as possibly involving PI!, there should be sufficient reason to believe that a security breech has occurred and that Pl! is likely to have been involved. Otherwise, the incident should be reporting following documented procedures for reporting all cyber security incidents.

Reports to CIAC may be made via email to ciac@ciac.org, by phone to 925-422-8193 or by fax to 925-423-8002.

CIAC will report the incident involving PU to the US-Computer Emergency Readiness Team (US-CERT).

7. RESPONSIBILITIES.

It is expected that Heads of Departmental Elements will be given delegated authority from the Deputy Secretary in the near future relative to detennining that data on mobile computers/devices are non-sensitive (Recommendation I in 0MB M-06-16).

8. REFERENCES.

References are defined in DOE CIO Guidance CS-!, ***Ma11agemel1t, Operational, and Technical Controls.***

9. DEFINITIONS.

Definitions specific to this Guidance are defined in Attachment 2. Acronyms and lenns applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS· 1, ***Management, Operational, and Technical Co!l/rols Guidance.***

to.CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT I

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-38 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chiefinformation Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office ofHmnan Capital Management
Office of the Inspector General
Office ofIntelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Scieuce
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT2

GLOSSARY

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

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, O.c. 20603

June 23, 2006

M-06-16

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Jolmson Ill VX
Deputy Director for Mana)ent

SUBJECT: Protection of Sensitive Agency Information

In an effort lo properly sa'rcguard our infonnation assets while using infonnation technology, it is essential for all departments and agencies to know their baseline of activities.

The National Institute of Standards and Technology (NIST) provided a checklist for protection of remote infonnation. (See attachment) The intent of implementing the checklist is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. In addition to using the NIST checklist, I am recommending ail departments and agencies take the following actions:

I. Encrypt all data on mobile computers/devices which catty agency data unless lhe data is detennined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4. Log all computer-readable data extracts from databases holding sensitive infonnation and verify each extract including sensitive data has been erased within 90 days or its use ls still required.

Most departments and agencies have these measures already in place. We intend to work with the Inspectors General community to review these items as well as the checklist to ensure we are properly safeguarding the information lhe American laxpayer has entrusted to us. Please ensure these safeguards have been reviewed and are in place wilhin the next 45 days.

Attachment

Security Checklist

Protection of "Remote" Information

This checklist provides specific actions to be taken by federal agencies for the protection of Personally Identifiable Information (Pll) categorized in accordance with FIPS 199 as moderate or high impact that is either:

- Accessed remotely; or
- Physically transported outside of the agency's secured, physical perimeter (this includes information transported on removable media and on portable/mobile devices such as laptop computers and/or personal digital assistants).

The specific intent is to compensate for !he protections offered by the physical security controls when information is removed from, or accessed from outside of the agency location. Additionally, this checklist has been developed from existing guidance with the expectation that information security is a mission requirement essential to achieving the operational benefits of information technology without exposing !he agency, its assets, or individuals to undue risk.

The security controls and associated control assessment methods/procedures in this checklist were taken from NIST Special Publication **800-53,** ***Recommel1ded Security Controlsfor Federal Infonnation Systems*** and NIST Special Publication 800-53A, ***·Guide for Assessinp the Security Controls in Federal Infonnalion Systems*** (Second Public Draft), April 2006. The controls and assessment methods/procedures in !he checklist are a subset of what is currently required for moderate and high impact information systems. However, the checklist does include specific guidance on the technology to be used for some controls.

References:

Federal Information Processing Standards Publication (FIPS) **199,** ***Sta11dardsfor Security Categorization of Federal Infonnation and Information Systems,*** February 2004.

NIST Special Publication **800-53,** ***Recommended Security Conrro/sfor Federal lnfonnation Systems,*** February 2005.

NIST Special Publication 800-53A, ***Guidefor Assessing tlle Security Controls in Federal Information Systems*** (Second Public Draft), April 2006.

---

[1] For purpose of this Se<.'.'.urity Checklist the assessment methods and procedures outlined in NfST Special Publication 800 53A (Second Public Dnd1), dated April 2006, are considered mandatory. Updated control assessment methods and procedures will be effective upon final -publication of Spe<:ial Publication 800 S3A.

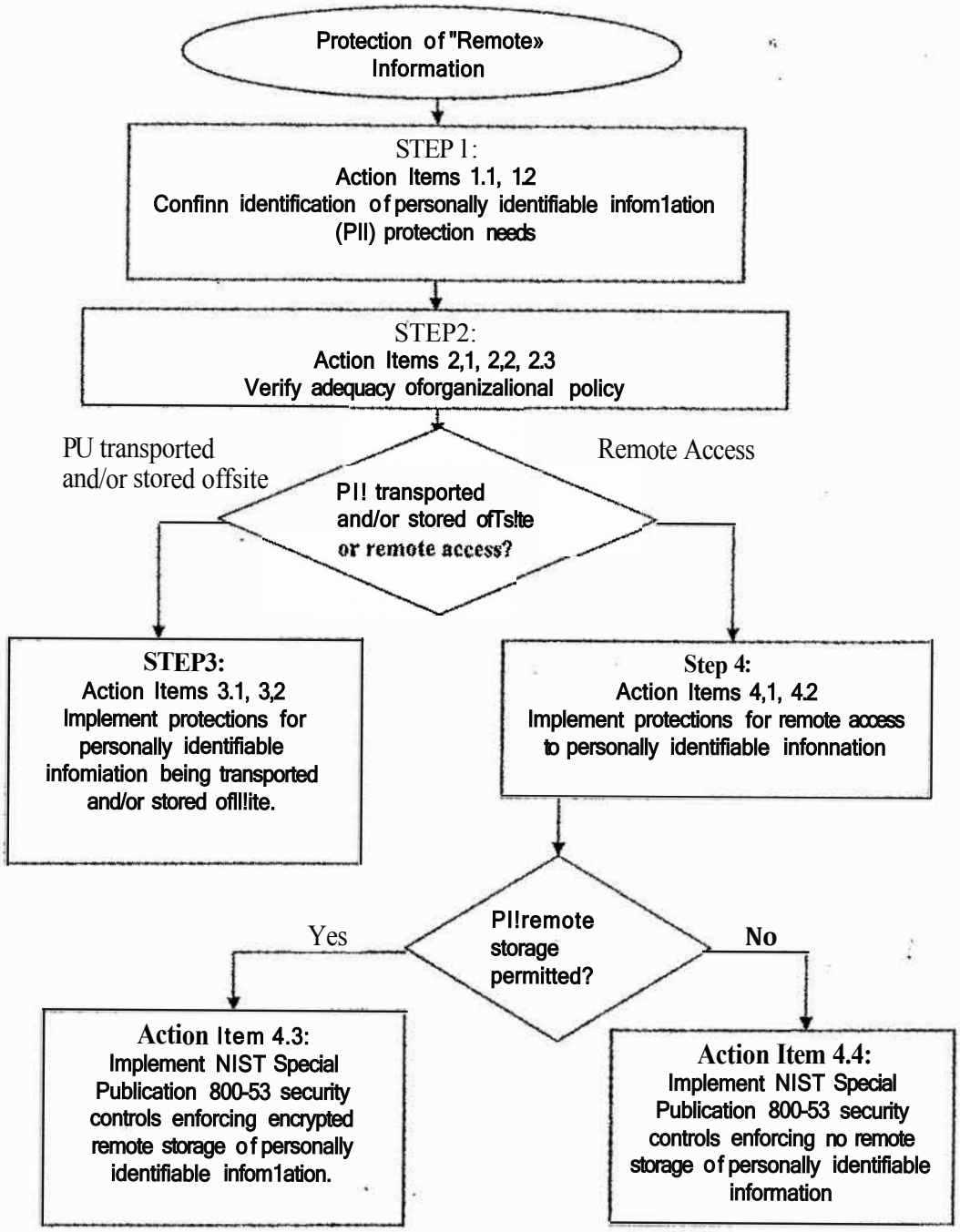


Figure: Process for Protection of "Remote" Infonnation

SECURITY CHECKLIST FOR PERSONALLY IDENTIFIABLE INFORMATION THAT IS TO BE TRANSPORTED AND/OR STORED OFFSITE, OR THAT IS TO BE ACCESSED REMOTELY

	Procedure
	[illegible] confirm ide[illegible] identifia[illegible]
	Action Item 1.1: Verify infomiation categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed.
	Action Item 1.2: Verify existing risk assessment.
	[illegible]
	Action Item 2.1: Identify existing organizational policy that addresses the infonnation protection needs associated with personally identifiable information that is accessed remotely or physically removed.
	Action Item 2.2: Verify that the existing organizational policy adequately addresses the infonnation protection needs associated with personally identifiable information that is accessed remotely or pbysically removed.
	Action ***Item 2.3:*** Revise/develop organizational policy as needed, including steps 3 and 4.
	If personally Identifiable information is to be transported and/or stored offsite, follow Step 3; for remote access to personally Identifiable information, follow Step 4.
	[illegible] protections for personally identifiable in[illegible] [illegible]ite.
	Action Item 3.1: In those instances where personally identifiable information is transported to a remote site, implement NIST Special Publication 800-53 security controls ensuring tbat information is transported only in encrypted fonn.
	Action ***Item 3.2:*** In those instances where personally identifiable information is being stored at a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is stored only in encrypted form.
	Checklist Complete.
	STEP 4: [illegible] Identifiable Information.
	Action ***Item*** *4.1:* Implement NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection.
	Action ***Item 4.2:*** Implement NIST Special Publication 800-53 security controls enforcing allowed downloading of peisonally identifiable information.
	If remote storage of personally identifiable information is to be permitted follow Action Item 4.3, otherwise follow Action Item 4.4.
	Action ***Item 4.3:*** Implement NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information.
	Checklist Complete.
	Action Item 4.4: Implement NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information.
	Checklist Complete.

Security Controls and Assessment Procedures

STEP 1: Confirm Identification of personally identifiable Information protection needs.

Action Item 1.1: Verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed.

Guidance: The purpose of this step is to review the FIPS 199 security categorization of organizational information with the focus on remote access and physical removal. The intent is to ensure all personally identifiable information through which a moderate or high impact might result has been explicitly identified. For example, databases where the loss, corruption; or unauthorized access to personally identifiable information contained in the databases could result in a serious adverse effect, with widespread impact on individual privacy being one area of specific concern.

Related SP 800-53 controls and associared SP 800-53A assessment procedures:

PL-S PRIVACY IMPACT ASSESSMENT

SP 800-53A: PL-5.1, PL-5.2 (for high impact add: PL-5.3, PL-5.4)

RA-2 SECURITY CATEGORIZATION

SP 800-53A: RA-2.1, RA-2.2, RA-2.3 (for high impact add: RA-2.4, RA-2.5)

Action Item 1.2: Verify existing risk assessment.

Guidance: The purpose of this step is to apply the results from the previous action item and operational experience to confirm or modify as needed the existing risk assessment associated with remote access and physical removal of personally identifiable information.

Related SP 800-53 controls and associated SP 800-53A assessmenr procedures:

RA-4 RISK ASSESSMENT UPDATE

SP 800-53A: RA-4.1, RA-4.2, RA-4.3 (for high impact add: RA-4.4, RA-4.5)

STEP 2: Verify adequacy of organizational policy.

Action Item 2.1: Identify existing organizational policy that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.

Guidance: This step is primarily to identify the existing policy related to the security and privacy needs associated with personally identifiable information accessed remotely or physically removed from agency-controlled areas.

Related SP 800-53 controls and associated SP 800-53A assessme1tlprocedures:

See action item 2.3.

Action Item 2.2: Verify that the existing organizational policy adequately addresses the **infonnation protection needs associated with personally identifiable infonnation that is accessed** remotely or physically removed.

Guidance: **Having determined which existing policy is applicable to the remote access or physical removal of personally identifiable infonnation, the purpose of this action item is to verify the adequacy of that policy. The policy should address the following specific questions:**

1. **For *Personally Iden/if/able lnformat/011* physically removed:**
   a. **Does the policy explicitly identify the rules for detennining whether physical removal is allowed?**
   b. **For personally identifiable infonnation that can be removed, does the policy require the information be encrypted and that appropriate procedures, training, and accountability measures are in place to ensure that remote use of this encrypted infonnation does not result in bypassing the protections provided by the encryption?**
2. **For *Personally Identifiable Information* accessed remotely:**
   a. **Does the policy explicitly identify the rules for detennining whether remote access is allowed?**
   b. **When remote access is allowed, does the policy require that this access be accomplished via a virtual private network {VPN) connection established using agency-issued authentication certificate{s) or hardware token?**
   c. **When remote access is allowed, does the policy identify the rules for detennining whether download and remote storage of the information is allowed? (For example, the policy could permit remote access to a database, b)lt prohibit downloading and local storage of that database.)**

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

See action item 2.3.

Action item 2.3: **Revise/develop organizational policy as needed, including steps 3 and 4.**

Guidance: **Based upon the results from the previous action items, the organizational policy is revised or developed to fully address the questions posed in the previous action items.**

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

SP 800-53A: AC:J.l, AC-l.2, AC-l.3, AC-1.4 (for high impact add: AC-1.5, AC-1.6, AC-I.7)

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

SP 800-53A: AT-LI, AT-1.2, AT-1.3, AT-1.4 (for high impact add: AT-1.5, AT-1.6, AT-1.7)

AU•l AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

SP 800-53A: AU-1.1, AU-1.2, AU-1.3, AU-1.4 (for high impact add: AU-1.5, AU-1.6, AU-1.7)

IA•l JDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

SP 800-53A: IA-1.l, IA-1.2, IA-1.3, IA-1.4 **(for** high impact **add:** IA-1.5, IA-1.6, IA-1.7)

MP•l MEDIA PROTECTION POLICY AND PROCEDURES

SP 800-53A: MP-LI, MP-1.2, MP-1.3, MP-1.4 **(for** high impact **add:** MP-1.5, MP-1.6, MP-1.7)

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

SP 800-53A: SC-1.l, SC-1.2, SC-1.3, SC- 1.4 (for high impact add: SC-1.5, SC-1.6, SC-1.7)

I fperso,ia/ly identifiable Information is to be transported and/or stored offiste, follow Step 3; for remote access to personally Identifiable Information, follow Step 4.

STEP 3: Implement protections for personally IdenlIflable information being transported and/or stored olfsite.

Action Item 3.1: In those instances where persenally identifiable information is transported lo a remote site, implement NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form.

Guidance: The intent is to apply the controls necessary to ensure that personally identifiable infonnation is appropriately encrypted prior lo being removed from the area under agency control.

Related SP 800-53 conlrals and associated SP 800-53A assessment procedures:

MP•S MEDIA TRANSPORT

SP 800-53A: MP-5.1, MP-5.2, MP-5.3 (for high impact add: MP-5.4, MP-5.5)

SC-13 USE OF VAl.lDATED CRYPTOGRAPHY

SP 800-53A: SC-13.1, SC-13.2 (for high impact add: SC-13.3, SC-13.4)

Action Item 3.2: In those instances where personally identifiable information is being stored at a remote site, implement NIST Special Publication 800-53 security controls ensuring that infonnation is stored only in encrypted fonn.

Guidance: Tiie intent is to apply the controls necessary to ensure that personally identifiable information remains appropriately enciypted during remote storage. This includes establishing and training users on the rules of behavior and infonnation use that will help prevent unencrypted forms of the infonnation from being stored on remote components oftlie information system,

Related SP 800-53 controls and associated SP 800-53A assessmentprocedures:

PL-4 RULES OF BEHAV!OR

SP 800-53A: PL-4.1, PL-4.2, PL-4.3, PIA.4, PL-4.5 (for high impact add: PL· 4.6, PL-4.7)

SC-4 INFORMATION REMNANTS

SP 800-53A: SC-4.1, SC-4.2 (for high impact add: SC-4.3, SC-4.4)

SC· 13 USE OF VALIDATED CRYPTOGRAPHY

SP 800-53A: SC-13.1, SC-13.2 (for high impact add: SC-13.3, SC-13.4)

STEP 4: Implement protections for remote access to personally Identifiable infonnation.

General Guidance: This step is executed when the policy allows remote access to personally identifiable infonnation.

Action Item 4.J: Implement NIST Special Publication 800-53 security controls requiring authenticated, virtual private network (VPN) connection.

Guidance: The intent is to apply those controls necessary to both mandate and achieve connections from remote components o fthe infonnation system to an internal agency network via a virtual private network (VPN). The VPN is established based upon authentication using agency-controlled certificates or hardware tokens issued directly to each authorized user.

Related SP 800-53 controls and associated SP 800-53A assessme11tprocedures:

AC-17 REMOTE ACCESS, with Enhancements (I), (2), and (3)

SP 800-53A: AC-17,l, AC-17.2, AC-17.3, AC-17.4, AC-17.5, AC-17.6, AC-17.7, AC-17.10, AC-17.11, AC-17.13, AC-17.15 (for high impact add: AC-17.8, AC-17.9, AC-17.12, AC-17.14, AC-17.16)

IA-5 AUTilENTICATOR MANAGEMENT

SP 800-53A: IA-5.1, IA-5.2, !A-5.3, IA-5.4, IA-5.5, IA-5.6 (for high impact add: IA-5.7, IA-5.8, IA-5.9)

Action Item 4.2: Implement NIST Special Publication 800-53 security controls enforcing allowed downloading o fpersonally identifiable infonnation.

Guidance: This action item ls executed when the policy allows personally identifiable information to be downloaded to a remote location. The intent is to apply controls necessary to enable and enforce only appropriate downloading. lncluded are controls for accessi$_{n\ g}$ only allowed infonnation, for least privilege (of downloaded information} necessary to perform duties, for what infonnation is allowed lo be transmitted across a remote connection, and for maintaining accountabilily for actions taken across the remote interface.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-3 ACCESS ENFORCEMENT, with Enhancement {I)

SP 800-53A: AC-3.1, AC-3.2, AC-3.3, AC-3.4, AC-3.7, AC-3.8.(for high impact add: AC-3.5, AC-3.6, AC-3.9)

AC-4 INFORMATIONFLOWENFORCEMBNT

SP 800-53A: AC-4.1, AC-4.2, AC-4.3 (for high impact add: AC-4.4, AC-4.5)

AC-6 LEAST PRIVILEGE

SP 800-53A: AC-6.1, AC-6.2, AC-6.3, AC-6.4 (for high impact add: AC-6.5, AC-6.6)

AC-13 SUPERVISION AND REVIEW - ACCESS CONTROL, with Enhancement (1) for high impact information

SP 800-53A: AC-13.l, AC-13.2, AC-13,3, AC-13.4 (for high impact add: AC-13.5, AC· 13.6, AC-13.7, AC-13.8, AC-13.9)

AU•2 AUDITABLE EVENTS

SP 800-53A: AU-2.l, AU-2.2, AU-2.3 (for high impact add: AU-2.4, AU-2.5)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING, with Enhancement (1) for high impact information

SP 800-53A: AU-6.l, AU-6.2, AU-6.3 (for high impact add: AU-6.4, AU-6.5, AU-6.6, AU-6.7)

I fremote storage o fpersonally identifiable information Is to be permitted follow Action Item 4,3, otherwise follow Action Item 4.4.

Action Item 4.3: Implement NIST Special Publication 800-53 security controls enforcing encrypted remote storage o fpersonally identifiable information.

Guidance: This action item is executed when policy allows personally identifiable information to be downloaded to a remote location. The intent is to apply those controls that both mandate and achieve encrypted storage o f the information at the remote location.

Related SP 800-53 co1ltrols and associated SP 800-JJA assessment procedures:

Pl 4 RULES OF BEHAVIOR

SP 800-53A: PL-4.l, PL-4.2, PL-4.3, PL4.4, PL-4.5 (for high impact add: PL-4.6, PL-4.7)

SC-4 INFORMATION REMNANTS

SP 800-53A: SC-4.l, SC-4.2 (for high impact add: SC-4.3, SC-4.4)

SC-13 USE OF VALIDATED CRYPTOGRAPHY

SP 800-53A: SC-13.1, SC-13.2 (for high impact add: SC-13.3, SC-13.4)

Action Item 4.4: Implement NIST Special Publication 800-53 security controls enforcing no remote stornge o fpersonally identifiable information.

Gilida1lce: This action item is executed when policy allows personally identifiable information to be remotely accessed only i fnot stored locally. The intent is to apply

those controls necessary to achieve remote use without local storage. The implementation of these controls will result in only necessary information being transmitted to the remote component of the information system. An example is transaction-based database access that provides no more information to the remote information system component than necessary for the immediate transaction. Another example is allowing downloading of only partial information to mitigate the risk by reducing the potential impact; for example, only extracts/views of a database or only views of statistical information.

Related SP 800-53 controls and associated SP 800-53A assessment procedures:

AC-3 ACCESS ENFORCEMENT, with Enhancement (1)

SP 800-53A: AC-3.1, AC-3.2, AC.3.3, AC-3.4, AC-3.7, AC-3.8 (for high impact add: AC-3.5, AC-3.6, AC-3.9)

AC-4 INFORMATION FLOW ENFORCEMllNT

SP 800-53A: AC-4.1, AC-4.2, AC-4.3 (for high impact add: AC-4.4, AC-4.5)

AC-6 LEAST PRIVILEGE

SP 800-53A: AC-6.1, AC-6.2, AC-6.3, AC-6.4 (for high impact add: AC-6.5, AC-6.6)

AC-13 SUPERVISION AND REVIEW-ACCESS CONTROL, with Enhancement (I) for high impact information

SP 800-53A: AC-13.1, AC-13.2, AC-13.3, AC-13.4 (for high impact add: AC-13.5, AC-13.6, AC-13.7, AC-13.8, AC-13.9)

AC-17 REMOTE ACCESS, with Enhancements (1), (2), and (3)

SP 800-53A: AC-17.1, AC-17,2, AC-17.3, AC-17.4, AC-17.5,AC-17.6, AC-17.7, AC-17.IO, AC-17.ll, AC-17.13, AC-17.15 (for high impact add: AC-17.8, AC-17.9, AC-17.12, AC-17.14, AC-17.16)

AT-2 SECURITY AWARENESS

SP 800-53A: AT-2.1, AT-2.2, AT-2.3 (for high impact add: AT-2.4, AT-2.5)

AU-2 AUDITABLE EVENTS

SP 800-53A: AU-2.1, AU-2.2, AU-2.3 (for high impact add: AU-2.4, AU-2.5)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING, with Enhancement (I) for high impact information

SP 800-53A: AU-6.1, AU-6.2, AU-6.3 (for high impact add: AU-6.4, AU-6.5, AU-6,6, AU-6.7}

PL-4 RULES OF BEHAVIOR

SP 800-53A: PL-4.1, PL-4.2, PIA.3, PL-4.4, PL-4.5 (for high impact add: PL-4.6, PL-4.7)

SC-4 INFORMATION REMNANTS

SP 800-53A: SC-4.1, SC-4.2 (for high impact add: SC-4.3, SC.4.4)

DOE Working Examples of Personally Identifiable Information (PII)
August 9, 2006

WHATISPU:

1. Social Security Numbers in any fonn are PII
2. Place of Birth associated with an individual
3. Date of birth associated with an individual
4. Mother's maiden name associated with an individual
5. Biometric record associated with an individual
    a. Fingerprint
    b. Iris scan
    c. DNA
6. Medical history infonnation associated with an individual
    a. Medical conditions, including history of disease
    b. Metric infonnation, e.g. weight, height, blood pressure
7. Criminal history associated with an individual
8. Employment history and other employment infonnation associated with an individual
    a. Ratings
    b. Disciplinary actions
    c. Perfonnance elements and standards (or work expectations) are PH when they are so intertwined with perfonnance appraisals that their disclosure would reveal an individual's performance appraisal.
9. Financial infonnation associated with an individual
    a. Credit card numbers
    b. Bank account numbers
10. Security clearance histcry or related information (Not including actual clearances held)

WHAT ISN'T PU:

1. Phone numbers (Work, Home, Cell)
2. Street addresses (Work and pl:)rsonal)
3. Email addresses (Work and personal)
4. Digital pictures
5. Birthday cards
6. Birthday emails
7. Medical information pertaining to work status (X is out sick today)
8. Medical information included in a health or safety report
9. Employment information that is not Pil even when associated with a name
    a. Resumes, unless they include an SSN
    b. Present and past position titles and occupational series
    c. Present and past grades

d. Present and past annual salary rates (including performance awards or bonuses, incentive awards, merit pay amount, Meritorious or Distinguished Executive Ranks, and allowances and differentials)
e. Present and past duty stations and organization of assignment (includes room and phone numbers, organization designations, work e-mail address, or other identifying information regarding buildings, room numbers, or places of employment)
f. Position descriptions, identification of job elements, and those performance standards (but not actual performance appraisals) that the release of which would not interfere with law enforcement programs or severely inhibit agency effectiveness
g. Security clearances held
h. Written biographies (like the ones used in pamphlets of speakers)
i. Academic credentials
    i. Academic credentials, e.g. Ph.D, MS, BS, AA
    ii. Schools attended
    iii. Major or area of study

10. Personal information stored by individuals about themselves on their assigned workstation or laptop (unless it contains an SSN)