DEPARTMENT OF HOMELAND SECURITY
SELF ASSESSMENT FOR PERSONNEL-RELATED DATA

The Under Secretary for Management and the Chief Privacy Officer have directed Components and Directorates to complete this self-assessment regarding the use and maintenance of personnel-related data by August 15, 2007. The Component/Directorate Head shall verify and confirm the accuracy of the information provided.

Personnel-related data is a subset of personally identifiable information (PII)[1] and includes any PII about DHS employees or contractors held in systems such as human capital operations, security operations, financial operations, time and attendance systems, user name and log in systems, travel systems, and any other electronic systems or hard copy records where such information may be found.

Personnel-related data is likely to be found throughout a Component/Directorate's operations, not only with those with programmatic responsibility for human capital and security operations, but also those in a management or supervisory role. Information may be both electronic and hard copy and can be at headquarters, regional, and remote locations.

Privacy security incidents can occur any time and any place, wherever appropriate safeguards have not been adhered to, and for this reason we are asking for Components and Directorates to examine the entire breadth of the organization, even down to the smallest office so that DHS is in a position to understand and identify possible issues before the next incident occurs.

Each Component/Directorate's cross functional team shall identify and review all paper-based and IT related programs that contain personnel-related data.

This self-assessment is divided into three separate sections:

- Questions regarding the policies and procedures in place for the entire Component/Directorate as it relates to the handling of personnel-related data. If DHS policies apply, you may also reference those.
- Questions regarding specific systems and programs using personnel-related data.
- Questions regarding all the facilities where these systems and programs are administered.

Upon completion and submission of this self-assessment and any supporting documentation that is relevant to the self-assessment, the Privacy Office, Human Capital Office, Office of Security, and Office of the Chief Information Officer will review the Component/Directorate's current handling policies and processes, and follow up with meetings to discuss the policies and procedures in place. This assessment will help ensure that previously issued policy has been implemented fully by the Component/Directorate or will help identify gaps in the

[1] "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, legal permanent resident, or a visitor to the U.S.

implementation. Based on the assessments and follow up meetings, the DHS team will develop Department-wide recommendations.

Please provide the self-assessments and any supporting documentation to Rebecca J. Richards, Director of Privacy Compliance, Privacy Office, email: pia@dhs.gov, by August15, 2007. For questions, please call the Privacy Office at 703-235-0780.

DEPARTMENT OF HOMELAND SECURITY COMPONENT/DIRECTORATE
PRIVACY SURVEY REPORT FOR PERSONNEL-RELATED DATA

This survey must be completed and any necessary supporting documentation relevant to the self-assessment for the overall privacy programs for personnel-related data provided as attachments. (DHS wide documentation does not need to be submitted, but Component/Directorate specific documentation does.)

Date submitted for review by DHS:				
Name of Component/Directorate:				
Name of Component/Directorate Contact:				
Email for Component/Directorate Contact:				
Phone number for Component/Directorate Contact:				
SPECIFIC QUESTIONS				
No.	**Description**	**Yes**	**No**	**N/A**
1	Does the Component/Directorate have policies and procedures related to the storage and maintenance of electronic and hardcopy personnel-related data? If yes, please provide a copy of Component/Directorate specific documentation and provide a reference to any applicable DHS-wide documentation.			
2	Does the Component/Directorate have policies and procedures related to sharing and exchange of electronic and hardcopy personnel-related data within and outside DHS? If yes, please provide a copy of Component/Directorate specific documentation and provide a reference to any applicable DHS-wide documentation.			
3	Does the Component/Directorate have policies and procedures related to the assignment and ongoing review of physical and electronic access to systems and files with personnel-related data? If yes, please provide a copy of Component/Directorate specific documentation and provide a reference to any applicable DHS-wide documentation.			
4	Does the Component/Directorate have policies and procedures related to the auditing of existing practices to ensure electronic and hardcopy data is handled in accordance with Component/Directorate and DHS privacy policies? If yes, please provide a copy of Component/Directorate specific documentation and provide a reference to any applicable DHS-wide documentation.			

5	Does the Component/Directorate have policies and procedures outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow rules regarding personnel-related data or more generally personally identifiable information or sensitive information? If yes, please provide a copy of Component/Directorate specific documentation and provide a reference to any applicable DHS-wide documentation.			
6	Describe the steps taken to implement the June 8, 2006 memo from the Chief Information Officer and Acting Chief Privacy Officer related to protecting personally identifiable information. <Please describe any steps taken to implement the protections described in the memo. Indicate completion dates for these steps.>			
7	How many programs handle personnel-related data in the Component/Directorate? <Please provide a number and a list of all programs, whether IT or paper-based that use or maintain personnel-related data.>			
8	How many programs have a PIA approved by the Chief Privacy Officer? <Please provide a number and a list of all programs, whether IT or paper-based that have an approved PIA. If PIA has not been approved, has a PTA been completed? If no, explain why.>			
9	How many programs have a DHS, Government-wide, or legacy System of Records Notice published in the Federal Register? <Please provide a number and a list of all programs, whether IT or paper-based that have a DHS SORN. If the program depends upon a Government-Wide SORN, provide that information. In all cases, provide the date and FR citation for the SORNs.>.			

DEPARTMENT OF HOMELAND SECURITY
PROGRAM PRIVACY SURVEY REPORT

This survey must be completed by each program or system that collects, uses, maintains, or stores personnel-related data. This form is a modified version of the Privacy Threshold Analysis (PTA) template.

Date submitted for review:	
Name of Program:	
Name of Component/Directorate:	
Name of Program Manager:	
Email for Program Manager:	
Phone number for Program Manager:	
SPECIFIC QUESTIONS	
No.	**Question**
1	**Describe the program and its purpose:** <Please provide a general description of the project and its purpose in a way a non-technical person could understand.>
2	**Status of Program:** ☐ This is a new development effort. ☐ This an existing project. Date first developed: Date last updated: <Please provide a general description of the update.>
3	**What information about individuals is collected, used, generated or retained?** <Please provide a specific description of information that might be collected, generated or retained such as names, addresses, emails, etc.>

4	**Is there a Certification & Accreditation record within OCIO's FISMA tracking system?** Please work with your Component/Directorate information security system manager (ISSM) to answer this question. ☐ Unknown. ☐ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

DEPARTMENT OF HOMELAND SECURITY
FACILITY SECURITY SURVEY REPORT

This survey must be completed by all facilities at which personnel-related data is collected, used, maintained, or stored.

Survey Conducted By: (Name, Position/Title and Phone Number)
Program Office of Surveying Official:
Date of Survey:
Address of Room/Area Surveyed: (Full Mailing Address)
Single or Multi-Tenant Facility: (If multi-tenant, list other government and non-government tenants)
Room Name and/or Number(s) Surveyed: (Identify specific number(s) and/or name of the room(s) surveyed)
Program Office Responsible for Surveyed Area:
Responsible Official for Surveyed Area: (Name, Position/Title and Phone Number)
Types of Personnel-Related Personally Identifiable Information (PII) Maintained by Surveyed Facility:
Types of Media Containing Personnel-Related PII Maintained in Surveyed Facility (Circle as applicable) **Network Server(s)** **Remote Access to Network Server(s) thru Desktop PC(s)**

Remote Access to Network Server(s) through Laptop(s)

Stand-alone PC (No Network Connection)

Stand-alone Laptop (No Network Connection)

Removable Media, e.g., Removable Hard-drive, CD, DVD, etc.

Paper hard-copies

Other (Explain):

No.	Description	Yes	No	N/A
1	Is access through the outer perimeter of the facility controlled during normal duty hours? Explain:			
2	If access through the outer perimeter is controlled: What are the means of control? Explain: What are the prerequisites for entry through the perimeter? Explain:			

	How are visitors, vendors, cleaning crew and other non-tenant personnel screened? Explain: What controls are in place for after-hours access? Explain:			
3	Does the facility have an active Building Security Committee? Explain:			
4	Is the perimeter of the facility, lobby, loading dock or other perimeter entrances, equipped with Closed Circuit Television (CCTV)? Explain: If Yes, is monitoring conducted in real-time and/or is information recorded? If recorded, how long is recorded information maintained? Explain:			

5	For multi-tenant facilities, is elevator/stairwell access to DHS space controlled during and after duty hours? Explain:			
6	Is direct access into all DHS space (to include individual rooms/areas) housing PII data controlled? Explain: Is equipment used for controlling access operational? Explain: Are keys, cards, or other devices for access issued to employees retrieved from the employee when no longer needed? Are combinations changed or removed from mechanical cipher locks when no longer needed? Explain:			

7	How are visitors, vendors, cleaning crew and other DHS and non-DHS personnel afforded access to DHS space (to include individual rooms/areas) housing PII data? Explain: Is their activity monitored while within DHS space? Explain:			

8	Do employees have the capability to secure media containing PII in a lockable container at their workstation or other area within the DHS space? Explain:			
9	Are printers/fax machines used to send/receive PII data located in an area where access is monitored? Explain:			
10	Are computer monitors displaying PII data positioned in such a manner as to prevent casual observation by persons without a need to know, or, turned off in the presence of persons without a need to know? Explain:			

11	Are employees allowed to remove portable storage devices containing PII data, e.g., laptops, removable hard-drives, CD's, DVD's, thumbdrives, etc., from the workplace? If yes, under what conditions is authority given and what controls are in place to ensure the integrity of the information and the device? Explain:			
12	What manner is used to dispose of/destroy media containing PII data? Explain: Are hard-copy documents containing PII data disposed of in regular trash or recycling bins? (PROHIBITED)			

Other Factors Affecting the Security of PII: