The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
privacy@dhs.gov
www.dhs.gov/privacy

December 30, 2008

PRIVACY POLICY GUIDANCE MEMORANDUM

Memorandum Number: 2008-02

MEMORANDUM FOR: DHS Directorate and Component Leadership

FROM: Hugo Teufel III
Chief Privacy Officer

SUBJECT: DHS Policy Regarding Privacy Impact Assessments

I. PURPOSE

This memorandum sets forth the policy defining when the Department of Homeland Security (DHS) Chief Privacy Officer conducts a Privacy Impact Assessment (PIA) of a program, technology, or information collection at DHS.

II. AUTHORITY

The DHS Chief Privacy Officer conducts PIAs under four specific statutory authorities. (1) Section 208 of the E-Government Act of 2002[1] requires PIAs of all information technology that uses, maintains, or disseminates personally identifiable information (PII) or when initiating a new collection of PII from ten or more individuals in the public. (2) Congress requires the Chief Privacy Officer to conduct PIAs on certain programs and activities of the Department. (3) Section 222(a)(4) of the Homeland Security Act of 2002, as amended,[2] authorizes the Chief Privacy Officer to conduct PIAs on rulemakings proposed by DHS. (4) Section 222(a)(1) of the Homeland Security Act authorizes the Chief Privacy Officer to ensure that technologies employed at DHS sustain, and do not erode, privacy protections.

III. PRIVACY POLICY

The Privacy Office conducts PIAs on technologies, rulemakings, programs, and activities, regardless of their type or classification, to ensure that privacy considerations and protections are incorporated into all activities of the Department in accordance with the Privacy Office's duties

[1] E-Government Act of 2002, Public Law 107-347; 44 U.S.C. Ch 36.
[2] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142.

under Section 208 of the E-Government Act, the Homeland Security Act, and other statutes, as applicable. Consistent with its statutory obligations, the Privacy Office conducts PIAs for the following policy reasons:

(1) **Informed Decision Making.** The PIA is designed to inform senior leadership and DHS program offices in their deliberations about how to implement privacy protections into new and existing programs. Senior leadership and program managers have the overall responsibility and commitment to ensure that DHS programs respect and protect privacy, but they may not have the privacy expertise necessary to evaluate how best to do so. The PIA helps them identify the privacy issues and evaluate whether activities have adequately addressed them.

(2) **Life Cycle Management.** The PIA ensures that privacy protections are built into a system during its development cycle. By regularly assessing privacy concerns during the development process, DHS ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).[3]

(3) **Transparency.** The PIA provides transparency to the public and external oversight bodies, including the Congress and the Government Accountability Office (GAO). PIAs serve to document publicly how privacy protections have been integrated into DHS operations and, in so doing, serve to build public trust and confidence in DHS programs.

(4) **Accountability.** The PIA serves as a foundation for accountability to oversight bodies both internal and external to DHS. It provides a benchmark by which oversight bodies including the DHS Office of Inspector General, the Office of Management and Budget (OMB), the GAO, and the Congress can evaluate DHS's programs for privacy compliance. For example, the Privacy Office works closely with the DHS Chief Information Security Officer to monitor and report to OMB on FISMA's privacy requirements. On a quarterly and annual basis, DHS reports to OMB its progress in conducting PIAs for information systems that are required to go through the FISMA Certification and Accreditation process. The Department's FISMA score, therefore, relies in part on conducting PIAs where applicable. In addition, all major DHS programs are reviewed annually to ensure that they have addressed privacy prior to their submission to OMB for inclusion in the President's annual budget.

The PIA process helps build the Fair Information Practice Principles (FIPPs), the Department's framework for privacy policy, into DHS activities that may have a privacy impact. This is

[3] Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, *et seq.*

consistent with the mandate in Section 222(a)(2) of the Homeland Security Act, which directs the Chief Privacy Officer to assure that "personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." The Privacy Office has developed various PIA templates that apply the FIPPs to different types of PIAs, including an E-Government Act PIA template and a rulemaking PIA template.

IV. IMPLEMENTATION

The DHS Chief Privacy Officer conducts seven categories of PIAs to implement the statutory authorities described above.

Standard Information Technology PIAs

Section 208 of the E-Government Act requires Federal agencies to complete PIAs prior to: (1) developing or procuring information technologies that collect, maintain, or disseminate PII; or (2) initiating, consistent with the Paperwork Reduction Act, a new collection of PII from ten or more individuals in the public.[4] OMB *Memorandum 03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* outlines the requirements of the Act. The DHS Privacy Office has also issued extensive guidance on PIAs in its *Privacy Impact Assessments: Official Guidance* and the accompanying PIA template, which are updated periodically.[5] The DHS Privacy Office has developed the Privacy Threshold Analysis (PTA) to help identify when an information technology system collects or uses PII and requires a PIA. The DHS Privacy Office requires every information technology system to complete a PTA as part of the Certification and Accreditation process.

The E-Government Act requires agencies to conduct PIAs on new and updated information technologies that affect PII, and to publish PIAs through agency websites, in the Federal Register, or by other means. Publication may be modified or waived for security reasons, or to protect classified, sensitive, or private information included in an assessment. DHS conducts the majority of its PIAs under the authority of this provision.

Rulemaking PIAs

Section 222(a)(4) of the Homeland Security Act directs the DHS Chief Privacy Officer to conduct PIAs on the Department's proposed rulemakings that affect PII. This authority is fairly unique in the Federal Government. It expressly augments the scope of the E-Government Act's PIA provision by recognizing the importance of considering the privacy impact of departmental

---

[4] Section 208 (b)(1)(A)(ii) of the E-Government Act builds upon the requirements of the Paperwork Reduction Act (PRA) (44 U.S.C. 3501 *et seq.*), by requiring a privacy impact assessment for the collection of PII from ten or more individuals other than agencies, instrumentalities, or employees of the United States. Federal agencies must obtain OMB approval and publish a notice in the Federal Register to conduct such a collection. In addition, under Section (e)(3) of the Privacy Act, when an individual is asked to supply information, notice is required on the form or on a separate form that can be retained by the individual. Privacy Act of 1974, 5 U.S.C. § 552a(e)(3).

[5] http://www.dhs.gov/xinfoshare/publications/gc_1209396374339.shtm

rulemakings that may or may not involve information technology systems. By conducting PIAs on DHS rulemakings that may impact privacy, the Privacy Office provides the Department with the opportunity to address privacy considerations during the rulemaking process. In addition, the public is informed through the PIA about how the proposed rule may impact privacy and how the Department proposes to address that impact. The public is then given an opportunity to provide comment on the proposed rule during the public comment period. The PIA for the Final Rule responds to the comments and addresses how privacy will be implemented in the new program or information collection.

Human Resource PIAs

The E-Government Act expressly excludes from its requirements systems that collect information solely about Federal employees.[6] Nevertheless, DHS considers its employees' privacy to be no less important than the privacy of the public. The failure to protect DHS employee information could erode the confidence of the public in DHS's ability to protect the public's information. Therefore, the Chief Privacy Officer conducts PIAs on information technology that collects and uses DHS employee or contractor information under its Homeland Security Act, Sections 222(a)(1) and (a)(2) authority. To date, the DHS Privacy Office has focused on conducting PIAs on human resource systems that affect DHS Headquarters, and/or any human resource system that affects two or more components.

National Security System PIAs

The E-Government Act also expressly excludes national security systems from its requirements.[7] Under Sections 222(a)(1), (a)(2), and (a)(4) of the Homeland Security Act, the DHS Privacy Office conducts PIAs on technology and programs that are classified, considered national security sensitive, or considered national security systems as defined by OMB M-03-22. PIAs are particularly critical for these programs because information about them is largely non-public. The PIA is a key component of ensuring that classified programs have appropriately considered and implemented privacy protections. These PIAs can serve as an internal deliberative tool as well as an internal oversight tool for national security activities that may receive less public scrutiny. These PIAs, however, often are not made public because of the deliberative nature of the documents, and because of national security concerns. In coordination with the affected

---

[6] E-Government Act of 2002 (Public Law 107-347) § (b)(1)(A)(ii)(II).

[7] E-Government Act of 2002 (Public Law 107-347) §§ 208(B)(iii) and (C). OMB M-03-22 basically adopted the definition of "national security system" used in the Clinger Cohen Act: a telecommunications or information system operated by the Federal Government, the function, operation, or use of which (A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons systems; or (E) is critical to the direct fulfillment of military or intelligence missions, but does not include a system used for routine administrative and business applications, such as payroll, finance, logistics and personnel management. (Clinger-Cohen Act of 1996, 40 U.S.C. 11103.)

component and the Office of the General Counsel, the Chief Privacy Officer may choose to publish a redacted, non-classified PIA, or choose not to publish the PIA due to those concerns.[8]

Program PIAs

In some instances, the Privacy Office conducts PIAs on programs or activities in which several information technology systems are used for a single purpose or where a program or activity raises privacy concerns related to the use of PII. In addition, the Privacy Office conducts PIAs when Congress mandates a PIA in conjunction with its funding of a specific program or activity.

Where a DHS program involves several information technology systems, one or more of which implicate Section 208 of the E-Government Act, it may be more appropriate to conduct a single PIA than to conduct a separate PIA on each of the information technology systems. Such a PIA provides a more holistic view of the privacy concerns related to a program, rather than a specific IT system, particularly where an individual may be interacting with multiple IT systems and the privacy concerns arise not from a specific system but from its use in combination with other systems. To ensure greater transparency and help build trust in DHS operations in these cases, a single PIA provides the public with a comprehensive view of a program's privacy impact and how the privacy concerns have been addressed.

Some programs may not fall under the E-Government Act but nevertheless raise privacy concerns related to the use of PII. In such cases, the Privacy Office may choose to conduct a PIA pursuant to Sections 222(a)(1) and (a)(2) of the Homeland Security Act in accordance with the criteria set forth below for privacy-sensitive technology. This implementation ensures that DHS privacy policies are incorporated into the program or activity.

Occasionally, Congress will require a PIA for a particular program that it has authorized or established. In these instances, the Privacy Office will conduct a PIA following its established policies and practices.

Privacy-Sensitive Technology PIAs

The Chief Privacy Officer may also conduct PIAs pursuant to authority under Section 222(a)(1) of the Homeland Security Act to assure that the use of technology sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information. The Privacy Office implements Section 222(a)(1) by conducting a PIA on any technology employed by DHS that involves PII, even where Section 208 of the E-Government Act may not otherwise apply. The Chief Privacy Officer exercises this authority judiciously and only where the public interest is served, based on the following factors:

---

[8] OMB M-03-22 states that "agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA)." OMB M-03-22, II(C)(3)(iii)(1); *see also* Section 208(b)(1)(C) of the E-Government Act.

1. The size and nature of the population impacted by the program, technology, or information collection.
2. The nature of the technology and, in particular, whether it is a new technology or has not been previously deployed by DHS or another Federal agency, or whether it presents unique or novel privacy considerations.
3. The use of the technology is high profile.

Pilot Testing

As described above, the DHS Privacy Office requires every information technology system to complete a PTA to identify those systems that collect or use PII and may require a PIA. Pilot testing may give rise to a PIA provided that the PTA has revealed that pilot testing will involve the collection or use of PII. Requiring programs using PII to conduct a PIA prior to pilot testing ensures that privacy protections are implemented throughout the program or system life cycle and that those privacy protections are configured while other changes are being contemplated. Of course, a PIA is required if Section 208 of the E-Government Act is implicated. If Section 222(a)(1) is implicated, a PIA is appropriate if, after weighing the factors listed in the section above, the Chief Privacy Officer determines that the public interest is served in doing a PIA. If DHS were to conduct a PIA on a system only after pilot testing was completed, the opportunity to implement efficient and meaningful privacy protections would be lost with a commensurate loss of resources and mission efficiency.