Privacy Impact Assessment
for the

Department Freedom of Information Act and Privacy Act Records Program

August 18, 2010

<u>Reviewing Official</u>
Mary Ellen Callahan
Chief Privacy Officer
and
Chief Freedom of Information Act Officer
Department of Homeland Security
(703) 235-0780

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

Abstract

The Department of Homeland Security (DHS) and its components (Department or DHS) have established a Departmental Freedom of Information Act (FOIA) and Privacy Act (PA) Program to maintain records created by the Department's FOIA and PA staff, as well as to manage a multitude of FOIA and PA systems. While DHS has established the Department's FOIA and PA program, some components have established information technology as well as paper-based systems designed to handle component-specific FOIA and PA processing. The purpose of the various systems within the FOIA and PA program is to process record requests and administrative appeals under the FOIA and PA, as well as access, notification, and amendment requests and appeals under the PA. These systems also maintain records used in litigation arising from such requests and appeals, and in assisting DHS in carrying out any other responsibilities under the FOIA and PA. The DHS Privacy Office has conducted this privacy impact assessment (PIA) to assess the risks presented by the use of personally identifiable information (PII) in the various FOIA and PA processes and systems employed by DHS' FOIA and PA program.

Introduction

The Freedom of Information Act of 1966, as amended (5 U.S.C § 552), permits any person to request access to federal agency records. The FOIA also establishes a presumption that records in the possession of federal departments and agencies are accessible to the people, except to the extent the records are protected from disclosure by any of nine exemptions contained in the law, or by one of three special law enforcement record exclusions.

The Privacy Act of 1974, as amended (5 U.S.C. § 552a), embodies a code of fair information principles that governs the collection, maintenance, use, and dissemination of PII by federal departments and agencies. Further, the PA permits U.S. citizens and legal permanent residents (LPRs) with the opportunity to request access to federal department and agency records that are maintained on an individual. As a matter of DHS policy, any PII that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a system of records subject to the Privacy Act, regardless of whether the information pertains to a U.S. citizen, LPR, visitor, or alien.[1] Individuals may request these records, except to the extent the records are protected from disclosure by exemptions contained in the laws.

The DHS FOIA and PA Disclosure Office, within the DHS Privacy Office, exists to promote transparency of Department operations and to serve as a leader in the federal community. Through this approach, the Office centralizes FOIA and PA operations to provide policy and programmatic oversight, and support implementation across the Department and to respond to individual requests for information under the FOIA and PA.

The Department uses its FOIA and PA systems to maintain records created by the Department's FOIA and PA staff. This includes the Department's FOIA and PA staff, including components, as well as staff of components who do not have a designated FOIA and PA office, but who do perform related

[1] *Available at:* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

functions. This framework captures the expansion of the overall FOIA and PA program and meets investigative, reporting, and other disclosure responsibilities related to the FOIA and PA. This program is the baseline for FOIA and PA activities, as led by the Chief Privacy Officer and Chief Freedom of Information Act Officer, for the Department.

Responsibility for responding to FOIA and PA disclosure requests at the Department falls under the purview of the Chief Privacy Officer, who serves concurrently as the Department's Chief Freedom of Information Act Officer. The Chief FOIA Officer exercises agency-wide responsibility for ensuring appropriate and effective compliance with disclosure laws, executive orders, regulations, and policies.

Officers and directors in the DHS FOIA and PA program, including in the components, are responsible for responding to FOIA and PA requests that are submitted to their respective components. These component FOIA and PA officers and directors report on matters relating to DHS FOIA and PA policy, oversight, and reporting through their component leadership and also coordinate closely with the Chief Privacy Officer and Chief Freedom of Information Act Officer.

No one information technology or paper-based system captures the Department's FOIA and PA processing procedures within DHS' FOIA and PA program. Some components utilize information technology, as well as paper-based systems, to receive, track, distribute, and respond to FOIA and PA requests. These information technology and paper-based systems may be government solutions, commercial products, or some mixture of both. Other components utilize common office software such as Microsoft Access, Microsoft Excel, and/or supplemented with other paper-based solutions.

Individuals submit FOIA and PA requests to the Department through various communications methods including U.S. mail, facsimile, e-mail, or via commercial shipping method. Once received, the Department's FOIA and PA staff records the request and then tasks it to the appropriate program office to conduct a search for the requested records. When an individual submits a request for records pertaining to an individual, PII provided by the requester may be used to assist the program office in conducting a search for the records. If records responsive to the request exist, they are analyzed for releasability and are enclosed with a letter to the requester itemizing the records and identifying what, if any, exemptions are claimed to withhold portions of the records either from the FOIA or PA. When no records exist that are responsive to the request, the component sends a letter to the requester advising them accordingly.

The Department's FOIA and PA program presents a series of privacy risks. This PIA will analyze these risks through a programmatic approach.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

Individuals submitting FOIA and/or PA requests to the Department provide PII with their request that varies depending on the substance of the request. Commonly, requestors may submit some or all of the following information with their FOIA and/or PA request, depending on the request:

- Name(s);

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

- Address(es) (business and personal);
- Phone Number(s) (business and personal);
- Email(s) (business and personal);
- Date of Birth;
- Place of Birth;
- Social Security Number;
- Alien Number;
- Attorney or representative's name;
- Attorney or representatives contact information; or
- Identifying characteristics and numbers of the records they are requesting such as "immigration application" or "human resources form."

DHS and its components receive FOIA and/or PA requests for Departmental records, which may contain Social Security Numbers. DHS does not request Social Security Numbers and requesters are not required to submit such information; such information is provided voluntarily by the requestor for identification purposes.

When the Department's FOIA and PA offices receive unsolicited correspondence from requesters, extraneous information is often submitted. It is incumbent on the respective FOIA and PA office to redact and protect that information as appropriate. The degree to which the Departments' FOIA and PA program protect necessary extraneous information varies depending on the amount of extraneous information provided and the component and system(s) utilized to process requests (see Question 1.7).

1.2 What are the sources of the information in the system?

Information is provided to the Department by: individuals who submit FOIA and/or PA requests; individuals who appeal DHS' denial of their FOIA and/or PA requests; individuals whose requests, appeals, and/or records have been referred to DHS by other agencies; and, in some instances, attorneys or other persons representing individuals submitting such requests and appeals, individuals who are the subjects of such requests, Department of Justice (DOJ) and other government litigators, and/or DHS personnel assigned to handle such requests or appeals.

Information provided to the Department for FOIA and/or PA requests is done voluntarily. FOIA and PA requestors are not required to submit any of the information recorded in the Department's systems, but without it, DHS may be unable to properly respond to requests.

Other sources of information sent to the Department's FOIA and PA program includes:

- Internal DHS components;
- Other federal agencies;
- Congressional offices;
- State and local governments;

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

- Foreign officials or governments;
- U.S. and foreign corporations;
- Non-government organizations, such as media or watchdog groups; or
- Others in the general public.

1.3 Why is the information being collected, used, disseminated, or maintained?

When individuals provide information to the Department for FOIA and/or PA requests, the Department uses this information to efficiently and accurately process record requests and administrative appeals under the FOIA and PA, as well as access, notification, and amendment requests and appeals under the PA. Also, the Department uses such information when defending itself in litigation arising from such requests and appeals; and in assisting DHS in carrying out any other responsibilities under the FOIA or PA including reporting requirements, such as the Annual FOIA Report to the U.S. Attorney General. The various systems within the Departments' FOIA and PA program are used to maintain these records.

1.4 How is the information collected?

Individuals provide information to the Department when submitting FOIA and/or PA requests. Requests are received by the Department via U.S. mail, electronic mail, facsimile, and various commercial shipping methods. This information is entered into the applicable FOIA and PA tracking system at the Department depending on where it was received. For example, at the DHS FOIA and PA Office, information is entered into the Internet Quorum (IQ)/Electronic Correspondence Tracking (ECT) System by:

- Scanning original documents into the ECT record as an Adobe PDF file;
- Typing the information received (manually) into the ECT record; and
- Copying information received electronically and pasting them into the appropriate fields in an electronic form which comprises a portion of the ECT record.

1.5 How will the information be checked for accuracy?

Information provided to the Department when submitting FOIA and/or PA requests is done so voluntarily. The requestor controls accuracy of the information. Information received by the Department from individuals submitting FOIA and/or PA requests is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. Should an inaccuracy be discovered during the resolution of the case file, the component handling the case file may contact the originating submitter for clarification.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

1.6 What specific legal authorities/arrangements/agreements define the collection of information?

The Department is authorized to collect information under the FOIA and PA per 5 U.S.C. § 301, § 552 (Freedom of Information Act), §552a (Privacy Act); 44 U.S.C. § 3101 (Records Management by Federal Agencies); and E.O. 12958 (Classified National Security Information, as amended). Pursuant to 5 U.S.C. § 301, DHS is authorized to implement Departmental regulations that manage DHS' day-to-day operations. These operations include regulating employees, managing agency business, and controlling agency papers and property.

The President's Transparency and Open Government Memorandum (January 21, 2009) and the OMB Director's Open Government Directive Memorandum (December 8, 2009) serve as further motivation for the Department's transparency and openness initiatives related to disclosure.

Information, including PII, within the DHS FOIA and PA program are collected, maintained, used, and disseminated in accordance with DHS/ALL-001 - Freedom of Information Act and Privacy Act Records System (October 28, 2009, 74 FR 55572).

1.7 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

Risk: There is a risk that an individual submitting a FOIA and/or PA request will submit more information than is necessary, such as a Social Security Number or A-Number, when submitting a disclosure request.

Mitigation: To mitigate this risk, the Department only requires certain information, such as name, date and place of birth, physical address and FOIA and/or PA request information when submitting a request. If more information is provided than necessary, the Department will redact and protect this information and will not enter the extraneous information into the applicable FOIA and PA system. This information will remain in the paper file but will not be further disseminated.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Information received by the Department from individuals submitting FOIA and/or PA requests are used strictly to analyze, process, and respond to the request. Once received, the Department's FOIA and PA staff records the request and then distributes it to the appropriate program office to conduct a search for the requested records. When an individual submits a request for records pertaining to an individual, PII provided by the requester may be used to assist the program office in conducting a search for the records. If records responsive to the request exist, they are analyzed for releasability and are enclosed with a letter to the requester itemizing the records and identifying what, if any, exemptions are claimed to withhold portions of the records either from the FOIA or PA. When no records exist that are responsive to the request, the component sends a letter to the requester advising them accordingly.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

The systems used by the Department's FOIA and PA staff are used to track the receipt, processing, and response of the request. Any analysis performed is done by an analyst and not a information technology system.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Information received by the Department from individuals submitting FOIA and/or PA requests is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. Should an inaccuracy be discovered during the resolution of the case file, the component handling the case file may contact the originating submitter for clarification.

Some FOIA and PA tracking systems used by the Department have data integrity checks built into the various systems. For example, a requester's address is verified against a U.S. Postal Service system for accuracy verification. Mistakes in the spelling of the writer's name, prefix, and/or suffix are corrected.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Risk: There is a risk of unauthorized or inadvertent release of personal information, as well as unauthorized browsing of information by FOIA and PA staff for unofficial purposes.

Mitigation: To mitigate this risk, the Department has:

- Restricted access to authorized personnel to record level privacy and security on specifically identified case folders;
- Limited access to selected groups only to their particularized functions rather than the whole of the data;
- Required the completion of appropriate access agreements for individuals requiring access to organizational information and information systems prior to authorizing access;
- Implemented physical access control devices on systems that display information to prevent unauthorized individuals from observing display output;
- Implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems;
- Employed a formal sanctions process for personnel failing to comply with established privacy and security policies and procedures; and
- Provided initial and follow-on privacy and security awareness training for each individual with access to FOIA and PA tracking systems.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Records pertaining to FOIA and/or PA requests are retained and disposed of in accordance with the National Archives and Records Administration's (NARA) General Records Schedule (GRS) 14. Files may be retained for up to six years. For requests that result in litigation, the files related to that specific litigation will be retained for three years after final court adjudication.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes, records pertaining to FOIA and/or PA requests are retained and disposed of in accordance with the NARA's GRS 14.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Records pertaining to FOIA and PA program are retained and disposed of in accordance with the NARA's GRS 14. This retention schedule is brief enough to ensure privacy protection, but long enough to ensure the operational integrity of the FOIA and PA program.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

Information received by the Department from FOIA and/or PA requestors, as well as information shared within the Department to ensure timely response to information requests consist of the Department's components, including:

- U.S. Citizenship and Immigration Services
- U.S. Citizenship and Immigration Services Ombudsman
- Office for Civil Rights and Civil Liberties
- U.S. Coast Guard
- Office of Counternarcotics Enforcement
- U.S. Customs and Border Protection
- Domestic Nuclear Detection Office
- Office of the Executive Secretary
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Office of the General Counsel
- Office of Health Affairs
- U.S. Immigration and Customs Enforcement
- Office of Inspector General
- Office of Intelligence and Analysis

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

- Office of Legislative Affairs
- Management Directorate
  - Office of the Chief Administrative Officer
  - Office of the Chief Financial Officer
  - Office of the Chief Human Capital Officer
  - Office of the Chief Information Officer
  - Office of the Chief Procurement Officer
  - Office of the Chief Security Officer
- Office of the Military Advisor
- National Protection and Programs Directorate
  - US-VISIT
- Office of Operations Coordination and Planning
- Office of Policy
- Privacy Office and Freedom of Information Act Office
- Office of Public Affairs
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Secret Service

4.2 For each organization, what information is shared and for what purpose?

Information may be shared, depending on FOIA and/or PA records requested with the components outlined in 4.1 to coordinate the Department's response to a FOIA and/or PA request and to ensure the most accurate response and accounting of records released. These components may share incoming and outgoing information, such as correspondence requests, documents related to DHS' response to requests, and documents relating to the appropriate handling and customer service actions required in response to requests.

4.3 How is the information transmitted or disclosed?

No one information technology or paper-based system captures the Department's FOIA and PA processing procedures within DHS' FOIA and PA program. Some components utilize information technology, as well as paper-based systems, to receive, track, task, and respond to FOIA and PA requests. These information technology and paper-based systems may be government solutions, commercial products, or some mixture of both. Other components utilize common office software such as Microsoft Access, Microsoft Excel, and/or supplemented with other paper-based solutions. All transmission of PII conforms with DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information.*

4.4 <u>Privacy Impact Analysis</u>: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Risk: There is a risk of unauthorized or inadvertent release of personal information, as well as unauthorized browsing of information by personnel for unofficial purposes.

Mitigation: To mitigate this risk, the Department has:

- Restricted access to authorized personnel to record level privacy and security on specifically identified case folders;
- Limited access to selected groups only to their particularized functions rather than the whole of the data;
- Required the completion of appropriate access agreements for individuals requiring access to organizational information and information systems prior to authorizing access;
- Implemented physical access control devices on systems that display information to prevent unauthorized individuals from observing display output;
- Implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems;
- Employed a formal sanctions process for personnel failing to comply with established privacy and security policies and procedures; and
- Provided initial and follow-on privacy and security awareness training for each individual with access to FOIA and PA tracking systems.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

The Department will only share information from within the FOIA and PA program with external organizations when required by statute, executive order, regulation, or policy and for the response of a FOIA and/or PA request. This coordination may be necessary to ensure that records requested, that are not DHS records, may be responded to by the applicable federal department or agency. External organizations do not have access to the Department's FOIA and PA information technology or paper based systems. Information may be shared with law enforcement, such as threatening correspondence directed at the Department or its employees, or if an opinion is sought from an attorney at DOJ on a particular matter of FOIA or PA law.

5.2 What information is shared and for what purpose?

The Department will only share information from within the FOIA and PA program with external organizations when required by statute, executive order, regulation, or policy and for the response of a FOIA and/or PA request. This includes information outlined in Section 1.1. This coordination may be necessary to ensure that records requested that are not DHS records may be processed by the applicable federal department or agency. External DHS organizations do not have access to the Department's FOIA and PA information technology or paper-based systems. Information may be shared with law enforcement, such as threatening correspondence directed at the Department or its employees, or if an opinion is sought from an attorney at DOJ on a particular matter of FOIA or PA law.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

5.3 How is the information transmitted or disclosed?

No one information technology or paper-based system captures the Department's FOIA and PA processing procedures within DHS' FOIA and PA program. Some components utilize information technology, as well as paper-based systems, to receive, track, task, and respond to FOIA and PA requests. These information technology and paper-based systems may be government solutions, commercial products, or some mixture of both. Other components utilize common office software such as Microsoft Access, Microsoft Excel, and/or supplemented with other paper-based solutions. All transmission of PII conforms to Departmental information handling guidance.

5.4 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Risk: There is a risk of unauthorized or inadvertent release of personal information, as well as unauthorized browsing of information by personnel for unofficial purposes.

Mitigation: To mitigate this risk, the Department has:

- Restricted access to authorized personnel to record level privacy and security on specifically identified case folders;
- Limited access to selected groups only to their particularized functions rather than the whole of the data;
- Required the completion of appropriate access agreements for individuals requiring access to organizational information and information systems prior to authorizing access;
- Implemented physical access control devices on systems that display information to prevent unauthorized individuals from observing display output;
- Implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems;
- Employed a formal sanctions process for personnel failing to comply with established privacy and security policies and procedures; and
- Provided initial and follow-on privacy and security awareness training for each individual with access to FOIA and PA tracking systems.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. If notice was not provided, why not?

Notice is provided through this PIA and DHS/ALL-001 - Freedom of Information Act and Privacy Act Records System (October 28, 2009, 74 FR 55572).

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Persons are not obligated in any way to submit FOIA and/or PA requests to the Department. If individuals do choose to submit a request, certain information is necessary to comply with requesting procedures for identification purposes as well as scope of request.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Persons are not obligated in any way to submit a FOIA and/or PA requests to the Department. If individuals do choose to submit a request, certain information is necessary to comply with requesting procedures for identification purposes as well as scope of request. The FOIA and PA program will work with the individual and collect only the limited amount of information necessary to respond to the request.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Notice is provided through this PIA and DHS/ALL-001 - Freedom of Information Act and Privacy Act Records System (October 28, 2009, 74 FR 55572). Risk is minimal because persons are not obligated in any way to submit a FOIA and/or PA requests to the Department. If individuals do choose to submit a request, certain information is necessary to comply with requesting procedures for identification purposes as well as scope of request.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals, partnerships, corporations, associations, or public or private organizations may request information pertaining to the FOIA and PA program as well as previously submitted FOIA and/or PA requests by submitting a FOIA and/or PA request. Please submit your request to: The Privacy Office and Freedom of Information Act Office, Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-00655, Washington, D.C. 20528-0550, or by facsimile at 703-235-0443 or via e-mail to foia@dhs.gov.

7.2 What are the procedures for correcting erroneous information?

Should an inaccuracy be discovered during the resolution of the request file, the component managing the request may contact the originating submitter. Additionally, FOIA and PA tracking systems and other automated systems have data integrity checks built into the system.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

If an individual believes or discovers that his/her information is inaccurate, he/she should write to: The Privacy Office and Freedom of Information Act Office, Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-00655, Washington, D.C. 20528-0550, or by facsimile at 703-235-0443 or via e-mail to foia@dhs.gov.

7.3 How are individuals notified of the procedures for correcting their information?

Notice is provided through this PIA and DHS/ALL-001 - Freedom of Information Act and Privacy Act Records System (October 28, 2009, 74 FR 55572).

7.4 If no redress is provided, are alternatives available?

If an individual believes or discovers that his/her information is inaccurate, he/she should write to: The Privacy Office and Freedom of Information Act Office, Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-00655, Washington, D.C. 20528-0550, or by facsimile at 703-235-0443 or via e-mail to foia@dhs.gov.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Procedures are provided through this PIA and DHS/ALL-001 - Freedom of Information Act and Privacy Act Records System (October 28, 2009, 74 FR 55572).

Also, if an individual believes or discovers that his/her information is inaccurate, he/she should write to: The Privacy Office and Freedom of Information Act Office, Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-00655, Washington, D.C. 20528-0550, or by facsimile at 703-235-0443 or via e-mail to foia@dhs.gov.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

Users of the Department's FOIA and PA program are outlined in Section 4.1.

8.2 Will contractors to DHS have access to the system?

Contractors do support the Department's FOIA and PA program and those components outlined in Section 4.1. Contractors support the disclosure function, as well as FOIA and PA information technology systems where they exist. As a condition of their contracted service with DHS, all contractors must:

- Sign a Non-Disclosure Agreement;
- Undergo a background investigation;

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

- Sign and acknowledge rules of behavior; and
- Sign and submit an access request form.

8.3 Does the system use "roles" to assign privileges to users of the system?

This PIA analyzes the Department's FOIA and PA program, which consists of multiple information technology and paper-based systems. No one system is being analyzed. Some components utilize information technology, as well as paper-based systems, to receive, track, task, and respond to FOIA and PA requests. In both cases, FOIA and PA tracking systems use role-based access control to assign privileges to users. Access to the information will be determined through specified role-based permissions, as authorized by the specific system owner. These role-based access controls are based upon the principal of least privilege. The principal of least privilege states that a user may only have the minimum privileges to perform their assigned tasks.

8.4 What procedures are in place to determine which users may access the system and are they documented?

Access to FOIA and PA systems is limited. Users are selected by component management based upon job function. A system user, functioning as a supervisor, may assign specific rights to other user to follow the case. For example, a supervisor who receives correspondence from a requester may choose to allow successive individuals to only view the document, but not to modify or delete the contents. When doing so, any access rights to the document must be specifically assigned to an individual user who receives the action.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

FOIA and PA information technology systems provide a complete audit trail that records all users' modifications and routing of records within FOIA and PA tracking systems.

FOIA and PA paper-based systems are monitored, managed, and audited by supervisors.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

FOIA and PA information technology systems provide a complete audit trail that records all users' modifications and routing of records within FOIA and PA tracking systems.

FOIA and PA paper-based systems are monitored, managed, and audited by supervisors.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

DHS components provide privacy training to all users, including contractors, of FOIA and PA systems. All users are expected to adhere to DHS Management Directive 11042.1, *Safeguarding*

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

Sensitive But Unclassified (For Official Use Only) Information. Users are trained on how to apply record level security to their work and when the application may be appropriate.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

This PIA analyzes the Department's FOIA and PA program, which consists of multiple information technology and paper-based systems. No one system is being analyzed. Some components utilize information technology, as well as paper-based systems, to receive, track, task, and respond to FOIA and PA requests.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Risk: There is a risk that malicious or inadvertent actions taken on a particular FOIA and/or PA request may not be traceable back to an individual.

Mitigation: To mitigate this risk, the Department has built in auditing controls for information technology systems whereby actions taken by a user on a case folder are tracked. This auditing feature maintains accountability of an action taken by an authorized user. Paper-based systems are monitored, managed, and audited by supervisors.

Risk: There is a risk that authorized individuals will have more permissions than required to perform their job function. This risk exists when any new user account is created.

Mitigation: To mitigate this risk, Department supervisors are responsible for reviewing the FOIA and PA programs permission matrix to ensure that programs are not allowing individual users' access to information that is not needed to complete necessary tasks, and that unauthorized individuals do not have access to information contained in the FOIA and PA programs.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

This PIA analyzes the Department's FOIA and PA program, which consists of multiple information technology and paper-based systems. No one system is being analyzed. Some components utilize information technology, as well as paper-based systems, to receive, track, task, and respond to FOIA and PA requests.

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

DHS has implemented strict access control measures for authorized users, record level security to protect designated case files, and an automatic timeout feature to prevent unauthorized browsing of the information contained within FOIA tracking systems.

9.3 What design choices were made to enhance privacy?

This PIA analyzes the Department's FOIA and PA program, which consists of multiple information technology and paper-based systems. No one system is being analyzed. Some components utilize information technology, as well as paper-based systems, to receive, track, task, and respond to FOIA and PA requests. Regardless of whether the system is an information technology system or a paper-based system, privacy is built in from the beginning.

Responsible Officials

Catherine Papoi
Deputy Chief FOIA Officer
and Director, Disclosure & FOIA
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
and Chief Freedom of Information Act Officer
Department of Homeland Security

AILA InfoNet Doc. No. 10090266. (Posted 09/02/10)