Privacy Impact Assessment
for the Department of Justice Blog

Office of Public Affairs

September 28, 2009

Contact Point
Tracy Russo
Office of Public Affairs
(202) 514-2007

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Nancy C. Libin
Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 307-0697

Introduction

The Department of Justice Blog ("Blog"), located on the Department of Justice's ("DOJ" or "Department") website, provides a mechanism for the Department to publish content related to the Department's missions and operations using the WordPress blog software in order to enhance the Department's ability to communicate with the public, as well as increase government transparency and promote public participation and collaboration. The Blog is intended to provide a platform for the DOJ to communicate with the public about the work of the DOJ using plain language and multimedia assets such as pictures, videos, and audio clips. The Blog may also link to other websites within and outside the DOJ.

The Department's Office of Public Affairs (OPA) is the office coordinating the publication of content on the Department's Blog. Specifically, the Blog editor, who works in OPA, is the only user with publication rights to post content for public dissemination on the Department's Blog. As such, the Blog editor and OPA will be responsible for ensuring that information published on the Blog is vetted and approved for public dissemination. Additionally, the Department has established an internal Web 2.0 policy working group to continue to review issues pertaining to the Department's use of the Blog in order to ensure that its uses are in accordance with applicable laws, regulations, and policies.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The system will contain content published on the Blog by the Department. The Department does not collect information from individuals who view the Blog.

1.2 From whom is the information collected?

Information in the published content on the blog comes from Departmental and other records on which the published content is based and from Departmental personnel and other related individuals who contribute to the published content.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The Department collects content in order to display the content on the Blog so that it will be available for public view.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The Department is authorized to maintain a Department Blog pursuant to 5 U.S.C. § 301 and 44 U.S.C. § 3101.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The system is designed in a manner that allows individuals to view the Blog without providing personally identifiable information.

The Blog editor is the only user permitted to publish content on the Department's Blog. The Blog editor is trained and is advised in the laws, regulations, and policies that pertain to the public disclosure of personally identifiable information by the Department. Accordingly, the Blog editor will be responsible for ensuring that any published content that includes personally identifiable information will be reviewed and approved for public dissemination. Because only the Blog editor is permitted to publish content on the Blog, the risks associated with unauthorized disclosure of personally identifiable information should be mitigated.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The Department will collect proposed content from a defined set of authorized contributing users within the Department, and the Blog editor will publish certain content on the Blog for public dissemination.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as "data mining".)

No.

3.3 How will the information collected from individuals or derived from the system, including the system itself, be checked for accuracy?

The content will be checked for accuracy prior to publishing as part of the review, editorial, and disclosure approval process.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

The Department retains the Department's published content, which may be based on existing Departmental records. In accordance with the Federal Records Act, the Department is currently developing a records retention schedule for information posted to the Blog.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The Department has established user groups, as defined in response to question 8.1, to ensure that the posting and publication of content is controlled by authorized users. Additionally, all Department employees and contractors receive privacy training annually in conjunction with computer security training. Department employees and contractors are required to acknowledge the General Rules of Behavior on an annual basis. Thus, the risk that an authorized user will improperly handle the information is mitigated by such measures.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Prior to publication, the content is contributed by a defined set of authorized users and shared with the system administrators and Blog editor.

4.2 For each recipient component or office, what information is shared and for what purpose?

As stated in response to question 4.1, the content prior to publication is contributed by a defined

set of authorized users and shared with the system administrators and Blog editor for review for public dissemination.

4.3 How is the information transmitted or disclosed?

Other than the proposed content for publication that is submitted by a defined set of authorized users, the content is not transmitted or disclosed prior to publication on the Blog.

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

Not applicable. Other than the submission of proposed content for publication to the system administrators and Blog editor, there is no internal sharing of the information from this system. Once the proposed content is submitted to be reviewed for publication on the Blog, the information is technically secured in accordance with Section 8.0 of this PIA.

Section 5.0
External Sharing and Disclosure

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

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Content published on the Blog is for public dissemination via the Department's website.

5.2 What information is shared and for what purpose?

The Department will share content published on the Blog with the public through the Department's website. The purpose of the Blog is to disseminate mission-related information to the public.

5.3 How is the information transmitted or disclosed?

The Department will share content published on the Blog with the public through the Department's website.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Because content published on the Blog is transmitted to the public through the Department's website, agreements concerning the security and privacy of this information would not be necessary.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

Not applicable. The information published on the Department's Blog is intended to be disseminated to the public and viewed on the Department's website. As such, no training is required to receive this information.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Not applicable. The information published on the Department's Blog is intended to be disseminated to the public, and viewed on the Department's website. As such, auditing the recipients' use of the information would be unnecessary.

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

Content published on the Blog will be reviewed to ensure that information is appropriate for public dissemination under applicable laws, including the Privacy Act and the Freedom of Information Act. As stated above, only the Blog editor is permitted to publish content on the Blog and, as such, will ensure that information that includes personally identifiable information is vetted and approved to be published for public dissemination. The Blog editor is trained and advised in such laws, regulations, and policies, and therefore, the privacy risks associated with unauthorized disclosure of personally identifiable information should be mitigated. In addition, the Department has established an internal Web 2.0 policy working group to review and resolve privacy issues that may arise with the Department's use of the Blog.

Section 6.0
Notice

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

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Prior to collecting information from individuals for publication on the Blog, the Blog editor and those personnel authorized to assist in the Blog editorial process will provide notice to such individuals that information that they provide may be published on the Blog. Additionally, the Blog editor and those personnel authorized to assist in the Blog editorial process will seek consent, when applicable, for public dissemination of the information provided. For example, if the Blog editor interviews an individual for a video profile to be published on the Blog, the Blog editor will provide notice to the interviewee that any information captured on the video may be published on the Blog. Additionally, the Blog editor shall obtain consent from such individual to publish any information from the video on the Blog for public dissemination. The Blog editor will ensure that not only the individual providing the information has been given notice and provided consent when applicable but that the content of the information that the individual provides is vetted and approved for public dissemination via the Department's Blog.

Additionally, the DOJ Blog may contain website links to non-DOJ websites. If a user chooses to click on the website link to view a non-DOJ website, the user will be provided with a notice that the user is leaving the DOJ's website and is accessing a non-DOJ website. Once a user leaves the DOJ website, the DOJ does not control the collection, use, or dissemination of information that may be involved in the operation of other websites.

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

Yes, individuals solicited for information may choose not to provide information to be published by the Blog editor.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

As stated above in Section 6.1, individuals solicited to provide content to be published on the Blog will have an opportunity to consent to the publishing of the information on the Blog when applicable.

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

Because notice will be provided to the individual that provides information to be published on the

Blog, the individual should be fully aware that information provided may be published for public dissemination. Additionally, the contents of the information provided by individuals will be vetted and approved for public dissemination prior to its publication by the Blog editor in accordance with applicable privacy laws, regulations, and policies.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Individuals who provided information to the Blog editor for publishing may contact the Blog editor to update, amend, or delete such information. As the information will be published on the Department's website, individuals may seek access to the information by viewing the website.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

For individuals who provide information to the Blog editor for publication, the Blog editor shall provide notice regarding access and amendment of information provided for publication to the Blog.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Not applicable.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Not applicable. Information published on the Blog is for public dissemination in order to provide mission-related information to the public. As such, the Blog is not intended to be used to take actions against individuals based on the information published.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

The E-Government Services Staff, Office of the Chief Information Officer, has established and implemented an account management process which includes account justification, access restrictions based on separation of duties and least privilege, strong authentication management, re-certification efforts, and audit management.

Three user groups have access to the DOJ Blog:

Administrator - Someone who has access to all the administration features, including management of accounts.

Editor - Someone who can publish posts and manage posts as well as manage other people's accounts and posts.

Contributor - Someone who can write and manage their posts but not publish posts.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes, one contractor is working on the DOJ Blog system. The contractor is:

Pragmatics, Inc.

7926 Jones Branch Road

Suite 711

McLean, VA 22101

Pragmatics has five staff members working on the DOJ Blog project. The major responsibilities of the Pragmatics staff are to provide application development support, account management, system documentation, application integration, configuration management, and Tier 3 application support.

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

Yes, see the response to question 8.1. Further, technical controls employed include implementing access controls (e.g., role-based access controls, account management procedures to include separation of duties, principle of least privilege, need-to-know, timely account disablement/deletion, and annual account recertification), defining, introducing, and enforcing identification and authentication mechanisms.

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

E-Government Services Staff has established and implemented an account management process

to include account justification, access restrictions based upon separation of duties and least privilege, strong authentication management, re-certification efforts, and audit management. In addition, information is secured through strong encryption both in storage and in transit. This process is currently documented in the Blog Access Control Procedures.

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

System users are granted system access based on their organizational roles and a need to know. User account access lists are periodically reviewed to ensure that access to data maintained by the Department is protected. Reviewing these user accounts ensures that no rogue or erroneous accounts exist.

All requests to establish new accounts or modify the privileges of an existing account are approved by a system owner. Rights and privileges required for the completion of duties associated with defined roles are documented and retained by the E-Government Services Staff.

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

The DOJ Blog system implements auditing measures and technical safeguards in accordance with DOJ and Federal requirements established to prevent unauthorized disclosure and subsequent potential misuse of data. These procedures include:

Implementing System Access and Password Management and Monitoring - auditing of account creation, password activation/disabling and/or modification, access date/time, object, and other event relevant information in accordance with NIST SP 800-53, AU-3, Content of Audit Records; and

Continuous Monitoring - automated mechanisms are used to integrate audit monitoring, analysis, and reporting for response to suspicious activities. Audit records are maintained for suspicious activity or suspected violations and are investigated and immediately reported to the proper Department and E-Government Services Staff for further action. Implementation of these activities is in accordance with NIST SP 800-53, AU-6, Audit Monitoring, Analysis, and Reporting.

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

All Department employees and contractors receive privacy training annually in conjunction with computer security training. In addition, Department employees and contractors are required to acknowledge the General Rules of Behavior annually. Finally, the Blog editor is trained and advised of the laws, regulations, and policies pertaining to the dissemination of personally identifiable information by the Department to the public to ensure that the published content of the Blog is properly approved for public dissemination.

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

The data is secured in accordance with FISMA requirements. Certification and Accreditation of the system was completed September 17, 2009.

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

Privacy risks for access and security controls include unauthorized disclosure and modification of personally identifiable information. Unauthorized disclosure risks are mitigated through establishment of appropriate roles for users, establishment of strong authentication mechanisms, execution of an annual re-certification, and implementation of audit mechanisms. Controls are validated throughout the C&A lifecycle and as risks are identified; they are mitigated via Plans of Action and Milestones. In general, information is protected by management, technical, and operational safeguards appropriate to the sensitivity of the information. Users are properly trained in the safeguarding of identifying information stored within and/or processed by the DOJ Blog.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes, in 2009, the DOJ Blog technology was reviewed to evaluate the major operating characteristics and features of the system. Competing technologies (commercial Blog software) were evaluated prior to the selection of the Word Press Blog. Criteria for selection were based upon functionality, security, and interoperability concerns that would allow for DOJ to achieve its mission requirements. The DOJ Blog will better support DOJ's mission and business needs by providing a more centralized organizational structure to manage risk, communications, system configuration, security, and governance.

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

Security and privacy requirements were analyzed based on FIPS-199 security categorization. FIPS-199 categorizes a system as High, Medium, or Low, depending on how important the function is to the agency. The result of that analysis was that the system was rated Low for Confidentiality, Medium for data integrity, and Low for availability. All security controls are

applied in accordance with this rating. Requirements regarding integrity, privacy, and security were assessed throughout the system development lifecycle to include tasks such as the product selection and acceptance testing, system categorization, risk assessment, requirements analysis, security testing and evaluation, and independent certification, as well as tasks that have developed and described the system architecture and configuration(s). The OCIO security team has been involved with each of these tasks and has taken the necessary steps to ensure that the DOJ Blog is progressing through the lifecycle in compliance with applicable Federal and DOJ security policies in these areas. Furthermore, the security team ensures that the C&A lifecycle progresses parallel to the DOJ Blog system development lifecycle to ensure that integrity, privacy, and security are analyzed and continuously monitored.

9.3 What design choices were made to enhance privacy?

The DOJ Blog architecture design choices, which included enhanced security, were made in part on the ability of the information system to conform to required security standards of the Department. Further, these design choices included compliance with DOJ Order 2640.2E, 2640.1 (or successor), and the associated IT Security Standards in the areas of identification, authentication, integrity, and monitoring.

The DOJ Blog system limits its data input and Blog postings to authorized personnel only. The DOJ provides government staff and assigned contractor personnel mandated privacy training on the use and disclosure of personal data. The DOJ follows ITSS procedures and policies to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuse.

The Department considered the risks to the system and the sensitivity of the data as a basis for selecting security safeguards to provide adequate system protection. The system provides the capability to securely authenticate users before allowing access to system resources, disables inactive sessions within a specified time period, and provides the capability to audit system activity. During system identification and authentication, the authenticator field is masked with asterisks.

Conclusion

The concluding section should inform the reader, in summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

The DOJ Blog system stores and transmits information that is intended to be viewed by the general public via the Department's website. The Department has developed a comprehensive security program employing management, operational, and technical security controls to effectively secure the DOJ Blog system and mitigate associated risks.

The DOJ Blog system maintains an appropriate level of privacy protection and security, in accordance with both Department and industry standards. By limiting the publication role to the Blog editor, who is trained and advised in privacy laws, regulations, and policies concerning the public dissemination of personally identifiable information by the Department, the risks associated with unauthorized disclosures have been minimized.

Responsible Official

_____/s/_____ Date 9/28/09

Tracy Russo
New Media Specialist

Office of Public Affairs
Department of Justice

Reviewing Official

_____/s/_____ Date 9/28/09

Vance Hitch
Chief Information Officer

Office of the Chief Information Officer
Department of Justice

Approving Official

_____/s/_____ Date 9/28/09

Nancy C. Libin
Chief Privacy and Civil Liberties Officer

Office of the Deputy Attorney General
Department of Justice