U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO)

Privacy Impact Assessment

Department of Commerce Email System (DOC-ES)

PTOH-001-00

August 10, 2010

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

As part of the Department of Commerce (DOC) sponsored Email Consolidation Project, the USPTO has agreed to host and support the DOC Office of the Secretary Email, Calendaring, Instant Messaging and Blackberry Services. Microsoft Exchange is used as the mail server solution while Microsoft Outlook and On-line Webmail Access (OWA) is used to access email. The DOC-ES system is used to facilitate internal and external communication for the DOC. Primary users of the DOC-ES include staff within the DOC Office of the Secretary (OSEC), Inspector General, and Office of the Chief Information Officer.

The DOC-ES servers hosted at USPTO facilities are supported by USPTO Information Technology (IT) staff. However, all security policy and procedures surrounding the support of the software and hardware are managed by the DOC. Currently, an Interagency Agreement (IAA) between DOC and USPTO is in place that documents the equipment necessary for the USPTO to host the E-Mail, Calendaring, Instant Messaging and Blackberry Mobile Devices of the OSEC. Per the IAA, all services, roles, and responsibilities required for the support and services of the DOC-ES will be outlined in a future cross-service agreement.

QUESTIONNAIRE

1. What information is collected (e.g., nature and source)?

The DOC-ES has the capability to contain personally identifiable information (PII) within the email, instant messaging, and calendaring capabilities. The messages sent to and from DOC-ES users has the ability to contain multiple data elements classified as PII data. To mitigate this, users of DOC systems, including the DOC-ES, must sign rules of behavior which documents the user's responsibility for protecting and maintaining data to the best of their ability.

The DOC-ES also stores DOC employee user account (i.e., username and password) information necessary for the functioning of email and calendars. Individuals may collect contact information (i.e., names, phone numbers, and office locations to a limited extent) in personal address books in order to facilitate personal business communications. DOC business location information such as email address, room number, and phone number, is also available to internal DOC users from other sources.

Also, user account information is redisplayed in the addressing section of the email system. This information is available from several sources at DOC and may include name, room, business phone number, and email address. DOC-ES is an internal system; however, email can be sent to users outside of DOC domain. Individuals may choose to store email related contact data about correspondents on their hard drives; but it is for individual, not group use.

2. Why is this information being collected (e.g., to determine eligibility)?

The DOC-ES is used solely to facilitate communications from users within DOC to other users within DOC and external persons. This communication can include any data type, including PII data. However, it is not a necessity of the system to collect the PII data. The PII data elements can be sent from any person outside of the domain to DOC users.

3. What is the intended use of information (e.g., to verify existing data)?

The data within DOC-ES is used to facilitate communications by DOC employees or contractors to and from internal users and external persons.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

The information contained within the DOC-ES can be shared with any persons internal to or outside of DOC with a valid email address.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

All users have the option of providing nothing more than an email address and name. It is at the user's discretion to provide any additional information. Since the purpose of DOC-ES is to facilitate email and meeting schedules, the use of this data is part of the authorized use for the system. In addition, users accessing DOC systems must acknowledge a warning banner stating their rights to privacy using the system. If any user declines, they will not be able to log into their system to access DOC-ES.

6. How will the information be secured (e.g., administrative and technological controls)?

The information in the DOC-ES is protected by a user identification/password combination that is issued only to authorized individuals. Additionally, connections to the servers and information are controlled through mechanisms such as firewalls, spam filters, and encrypted tunnels. There is also a Service Level Agreement (SLA) between USPTO and DOC/OS which is renewed annually and requires that the signatories adhere to the National Institute of Standards and Technology (NIST) information security standards.

The system is currently undergoing a Security Authorization, as defined in OMB Circular A-130. The Security Authorization is the process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect IT systems and data stored in and processed by those systems. It is a process that encompasses the system's operation and ensures that the risk of operating a system is recognized, evaluated, and accepted.

The DOC-ES adheres to the standards in the Department of Commerce IT Security Program Policy and Minimum Implementation Standards; Appendix III, Security of Automated Information Resources, OMB Circular A-130; the Computer Security Act; and P.L. 107-347, Federal Information Security Management Act (FISMA).

7. How will the data extract log and verify requirement be met?

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

a. Who performed the extract,
b. When extract was done,
c. What was the extract,
d. Where was the extract taken from,
e. Has the extract been deleted and,

f. If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

A separate system of records notice (SORN) will not be developed for the DOC-ES. The data contained with DOC-ES can be covered under existing SORNs in place for DOC systems. Completed SORNs for DOC system can be located at http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/index.htm.

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

No, a separate system of records notice (SORN) will not be developed for the DOC-ES.

SIGNATORY AUTHORITY

/s/ Erin P. Fitzgerald — 8/24/2010

Agreed: _____ _____/_____/_____

Erin Fitzgerald — Date

DOC, Information System Owner

/s/ Theresa M. Schenk — 8/19/2010

Agreed: _____ _____/_____/_____

Theresa Schenk — Date

USPTO, Information System Owner

/s/ Rod Turk — 9/1/2010

Agreed: _____ _____/_____/_____

Rod Turk — Date

Senior Agency Information Security Officer

/s/ Wayne S. Blackwood — 8/25/2010

Agreed: _____ _____/_____/_____

Wayne Blackwood — Date

DOC, Co-Authorizing Official

/s/ John B. Owens II — 9/9/2010

Agreed: _____ _____/_____/_____

John B. Owens II — Date

USPTO, Co-Authorizing Official