# Federal Bureau of Prisons

# Privacy Impact Assessment
# for the
# Correspondence Tracking System (CTS)

**Issued by:**
**Sonya D. Thompson**
**Sr. Deputy Assistant Director/CIO**

| | |
|---|---|
| Reviewed by: | Luke J. McCormack, Chief Information Officer, Department of Justice |
| Approved by: | Joo Y. Chung, Acting Chief Privacy and Civil Liberties Officer, Department of Justice |
| Date approved: | September 25, 2013 |

# Section 1: Description of the Information System

The Federal Bureau of Prisons (BOP) protects society by confining offenders in the controlled environments of prisons and community-based facilities that are safe, humane, and appropriately secure, and that provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

As required by Section 208 of the E-Government Act, the BOP has prepared this Privacy Impact Assessment (PIA) for its Correspondence Tracking System (CTS) to describe information in identifiable form (IIF) maintained in the system and explain how the BOP uses and safeguards that information. The CTS application serves as BOP's central system for tracking and logging correspondence received at BOP facilities from external entities such as the federal judiciary, members of the U.S. Congress, federal and state agencies, and members of the public. Correspondence may include a variety of topics such as inquiries relating to a particular inmate (his/her medical care, conditions of confinement or sentence computation/release) or a specific BOP program (drug treatment, treaty transfer, etc.).

A letter (or copy of an email) is logged into the system, assigned a tracking number, assigned to a BOP program area or site for review and response, and then closed out after a response has been provided. The system may contain incidental IIF that has been voluntarily included in correspondence, such as the name of the correspondent, the mailing and email addresses of the correspondent, and any other personal information.

Users of this system are generally administrative officers and secretaries for Division, Regional, or Warden's Offices. Information can be retrieved from the system by entering either the assigned tracking number (e.g., DOJ Control number, BOP Control number, etc.), correspondent name, inmate register number, or issue cited. Users can also filter data based on the user who entered the correspondence item into the system or sort by date (e.g., the date of the letter, the date the letter was entered, or the date the item was closed).

The CTS application is web-based and authorized users access a common login portal using a browser. A network user ID and password are required and authentication occurs against the Lightweight Directory Access Protocol (LDAP). Access to data is controlled by group management and only users in the specified Business Process Management (BPM) CTS group may access the data. Communications and transmissions are encrypted using Secure Sockets Layer (SSL). The CTS application is an internal BOP system and is not interconnected with any outside system. Further, the CTS application is part of BOP's BPM software platform, which is a framework used to provide rapid application development of various minor BOP applications, like CTS.

# Section 2: Information in the System

## 2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

| General personal data | | | | | |
|---|---|---|---|---|---|
| Name | X | Date of birth | | Religion | |
| Maiden name | | Place of birth | | Financial info | |
| Alias | | Home address | X | Medical information | |
| Gender | | Telephone number | | Military service | |
| Age | | Email address | X | Physical characteristics | |
| Race/ethnicity | | Education | | Mother's maiden name | |
| Other general personal data (specify): X The personal data checked above includes the most frequently provided information included in correspondence to BOP. | | | | | |

| Identifying numbers | | | | | |
|---|---|---|---|---|---|
| Social Security | | Alien Registration | | Financial account | |
| Taxpayer ID | | Driver's license | | Financial transaction | |
| Employee ID | | Passport | | Patient ID | |
| File/case ID | X | Credit card | | | |
| Other identifying numbers (specify): X Inmate Register Number if provided by the author. | | | | | |

| Work-related data | | | | | |
|---|---|---|---|---|---|
| Occupation | | Telephone number | | Salary | |
| Job title | | Email address | | Work history | |
| Work address | | Business associates | | | |
| Other work-related data (specify): | | | | | |

| Distinguishing features/Biometrics | | | | | |
|---|---|---|---|---|---|
| Fingerprints | | Photos | | DNA profiles | |
| Palm prints | | Scars, marks, tattoos | | Retina/iris scans | |
| Voice recording/signatures | | Vascular scan | | Dental profile | |
| Other distinguishing features/biometrics (specify): | | | | | |

| System admin/audit data | | | | | |
|---|---|---|---|---|---|
| User ID | X | Date/time of access | X | ID files accessed | |
| IP address | | Queries run | | Contents of files | |

| System admin/audit data | |
|---|---|
| Other system/audit data (specify): | |

| Other information (specify) | |
|---|---|
| X | Issues identified in the letter based on pre-defined categories, such as inmate visitation, legal issues, religious matters, mental or medical health, etc. |
| | |
| | |

## 2.2 Indicate sources of the information in the system. (Check all that apply.)

| Directly from individual about whom the information pertains | | | | | |
|---|---|---|---|---|---|
| In person | | Hard copy: mail/fax | X | Online | |
| Telephone | | Email | X | | |
| Other (specify): | | | | | |

| Government sources | | | | | |
|---|---|---|---|---|---|
| Within the Component | | Other DOJ components | X | Other federal entities | X |
| State, local, tribal | X | Foreign | X | Embassies and government agencies | |
| Other (specify): X | Correctional organizations such as Association of State Correctional Administrators, (ASCA), American Correctional Association (ACA) and Joint Commission (health care accreditation entity). | | | | |

| Non-government sources | | | | |
|---|---|---|---|---|
| Members of the public | X | Public media, internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): | | | | | |

## 2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information

**from sources other than the individual, explain why.)**

The system is used only for internal purposes and the BOP maintains safeguards described in this PIA to protect this information. Privacy risks arise primarily from internal threats to the information contained within the CTS database, which include the unauthorized or inadvertent release of IIF and unauthorized browsing for information. To mitigate this risk, staff members are trained annually in IT security, including how to properly handle sensitive information. Staff members are also required to undergo information security awareness training prior to gaining access to the BOP network. Access to the system is limited to users who have an appropriate security clearance. Both user access and security clearance status are regularly reviewed.

Further, the system includes design choices that ensure that privacy protections exist for the sensitive information stored in the system. For example, role-based management is used to limit access to the system to authorized users. In addition, the system has a session timeout feature to protect against unauthorized viewing on unattended workstations. Privacy concerns were addressed at the maintenance, rather than collection, stage because IIF is included voluntarily by some requestors, so its presence in the system is a result of incidental collection. Considerations were also made regarding the security and protection of such data to ensure that the system complies with applicable privacy regulations and requirements for the protection of sensitive data. For example, data transmission is encrypted end-to-end during user sessions, data is regularly backed up, and access to the system requires the use of a user identification and strong password.

Also, information is safeguarded in accordance with BOP rules and policies governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, as well as the required use of proper user identification and passwords to access the system. Data transmission is also encrypted. The CTS application is an internal BOP system and is not interconnected with any outside system.

# Section 3: Purpose and Use of the System

## 3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

| Purpose | | | |
|---|---|---|---|
| | For criminal law enforcement activities | | For civil enforcement activities |
| | For intelligence activities | X | For administrative matters |
| | To conduct analysis concerning subjects of investigative or other interest | | To promote information sharing initiatives |
| | To conduct analysis to identify previously unknown areas of note, concern, or pattern. | | For administering human resources programs |
| | For litigation | | |
| | Other (specify): | | |

## 3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

CTS is used to track correspondence received by the BOP or referred to the BOP by the Department of Justice, other federal and state agencies, and other outside entities (e.g., foreign governments, private organizations, and members of the public). The system logs the inquiries and the actions taken by the BOP in response. The system is used to ensure the efficient, accurate, and timely handling of correspondence by the BOP and its numerous offices, as well as the timely retrieval of tracking information by the BOP. In addition, it also serves as a reference source for inquiries and responses thereto made by entities described in section 4.1 below.

## 3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

| Authority | | Citation/Reference |
|---|---|---|
| X | Statute | 5 U.S.C. 301 and 44 U.S.C. 3101. |
| | Executive Order | |
| | Federal Regulation | |
| | Memorandum of Understanding/agreement | |
| | Other (summarize and provide copy of relevant portion) | |

## 3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records are to be retained and destroyed in accordance with the schedules and procedures issued or approved by the National Archives and Records Administration (NARA). Records contained in CTS are scheduled under GRS-23, "Records Common to Most Offices Within Agencies, (8) Tracking and Control Records:" "Destroy or delete when 2 years old, or 2 years after the date of the latest entry, whichever is applicable." N1-GRS-98-2 item 45.

### 3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Access to the system is limited to users who have an appropriate security clearance and are authorized to review the information in the system as part of their official duties. User access privileges are regularly reviewed and users undergo a review of their security clearance every five years. Access is granted on a "least privilege" basis, controlled by BOP's centralized directory authentication model (i.e., users are only granted access to the information necessary to do their jobs and each login is checked to ensure that the user's account is valid and active). All access requests are processed, routed, and logged in BOP's helpdesk ticketing system for proper approval and auditing. Information in the system is safeguarded in accordance with BOP rules and policy governing automated information systems security. System transaction errors and exceptions are logged and reviewed on a routine basis. Data edit checks are included in program code to ensure appropriate and accurate entry of data. Staff members are routinely trained on the use and handling of information in the system, including annual training on information security and handling of sensitive information.

## Section 4: Information Sharing

### 4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | Case-by-case | Bulk transfer | Direct access | Other (specify) |
| Within the component | X | | X | |
| DOJ components | X | | | Administrative claims or investigations. |
| Federal entities | X | | | Congressional and Judicial Inquiries. |
| State, local, tribal gov't entities | X | | | Correctional entities; state criminal justice and civilian agencies. |
| Public | X | | | Inmate family or citizen inquiries. |
| Private sector | X | | | Media inquiries. |

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | Case-by-case | Bulk transfer | Direct access | Other (specify) |
| Foreign governments | X | | | Inquiries by embassies and consulates on behalf of constituent inmate. |
| Foreign entities | | | | |
| Other (specify): | | | | |

**4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)**

No private data is shared in the context of the response to an inquiry unless the subject of the IIF (e.g., the inmate) consents to its disclosure to a third party or the disclosure is made pursuant to a "routine use" under the applicable Systems of Records Notice (SORN) identified in Section 7 below. For instance, applicable routine uses include disclosures made for law enforcement and court-related purposes such as investigations, possible criminal prosecutions, civil court actions, or regulatory or parole proceedings.

To prevent or mitigate threats to privacy in connection with such disclosures, BOP staff reviews rules and procedures (what information may be disclosed, how it may be disclosed, how privacy data is to be protected, etc.) regarding access and use of the information via annual information security awareness training. Access to the system is also restricted to authorized users only.

## Section 5: Notice, Consent, and Redress

**5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)**

| | | |
|---|---|---|
| X | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. | |
| | Yes, notice is provided by other means. | Specify how: |
| | No, notice is not provided. | Specify why not: |

## 5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

| | | |
|---|---|---|
| X | Yes, individuals have the opportunity to decline to provide information. | Specify how: Any private information provided is done so voluntarily by the inmate directly or with the inmate's consent. |
| | No, individuals do not have the opportunity to decline to provide information. | Specify why not: |

## 5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to consent to particular uses of the information. | Specify how Individuals have the opportunity to consent to any certain disclosures unrelated to the routine uses specified in the SORN in Section 7.1 below: If the request for information is non-routine and the inmate has not previously provided consent, the inmate will be contacted to notify him/her of the request and determine if they consent to the disclosure. The inmate can decline access to the information. Examples of non-routine use would be a reporter requesting access to an inmate's discipline records; a member of the public who is seeking copies of inmate medical records via a FOIA request; or an inmate seeking access to the criminal history records of a fellow inmate. |
| X | No, individuals do not have the opportunity to consent to particular uses of the information. | Specify why not: Individuals do not have the opportunity to consent to routine uses of the information; (e.g., disclosure to law enforcement personnel for investigative purposes, disclosures pursuant to judicial inquiry, etc.). |

### 5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Any information provided, including IIF, that may be stored in the system is an incidental part of the individual's voluntary inclusion of such information in the applicable correspondence directed to BOP. Notice of routine uses and records access procedures are provided by the applicable System of Records Notices discussed in Section 7 below. No further notice is provided because BOP is not soliciting information from individuals; rather, individuals and other agencies make an initial request from BOP for information. Further, the general public is not obligated in any way to submit correspondence to BOP. Individuals have a right to decline sending information to BOP.

## Section 6: Information Security

### 6.1 Indicate all that apply.

| | |
|---|---|
| X | The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: January 2013<br><br>If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: |
| X | A security risk assessment has been conducted. |
| X | Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify:<br>Authentication occurs via unique userID identifications and passwords; change management is tracked and logged; session inactivity timeouts are implemented; and system maintenance activities are logged. |
| X | Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:<br>Documentation is audited during BOP program review and external audits. Access to certain sensitive information requires specific authorization and is limited to select personnel. |
| X | Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:<br>User access is audited as part of internal and external reviews. |
| | Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act. |

| | | | |
|---|---|---|---|
| | Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy. | | |
| X | The following training is required for authorized users to access or receive information in the system: | | |
| | X | | General information security training |
| | X | | Training specific to the system for authorized users within the Department. |
| | | | Training specific to the system for authorized users outside of the component. |
| | | | Other (specify): |

### 6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

System roles are assigned, and privileges to view data are based on such roles. User access for an employee must be requested by an appropriate supervisor, who confirms that access is required for the performance of his or her duties. The request and subsequent access is documented in the BOP HelpDesk system. Review and input of data is technically restricted to those that are involved in the correspondence tracking process or have a "need to know."

Users receive training on the potential for sensitive data to be included within the system and are continuously reminded about the need to strictly control the viewing and/or output of data from the system. BOP users are trained annually regarding the handling of sensitive information and information security requirements. All employees who are involved in the management, operation, programming, maintenance, or use of any DOJ information system are made aware of the threats and vulnerabilities of those systems and their responsibilities with regard to protecting privacy and information security. The Information Security Programs Office is responsible for providing the information on security requirements, procedures, and configuration management necessary to conduct the initial briefings for all users.

## Section 7: Privacy Act

### 7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

| | |
|---|---|
| **X** | Yes, and this system is covered by an existing system of records notice.<br><br>Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system:<br><br>• DOJ-003, Correspondence Management Systems for the Department of Justice; Corrections 66 FR 29992 (06/04/01); amended 66 FR 34743 (06/29/01); amended 67 FR 65598 (10/25/02); and further amended 72 FR 3410 (01/25/07). |

| | |
|---|---|
| | Yes, and a system of records notice is in development. |
| | No, a system of records is not being created. |

## 7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information can be retrieved from the system using the assigned tracking number (e.g., DOJ Control number, BOP Control number, etc.), correspondent name, inmate register number, or issue cited. Users can also filter data based on the user who entered the correspondence item into the system or by date (e.g., date of the letter, date the letter was entered into the system, or date the item was closed).