Federal Bureau of Prisons

Privacy Impact Assessment
for the
The Volunteers Influencing Inmate Outcomes System (VIIOS)

Issued by:
Sonya D. Thompson, SCOP

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [March 9, 2022]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Volunteers at the Federal Bureau of Prisons (BOP) provide an array of services to support the rehabilitative efforts of inmates, including the transition of inmates from BOP institutions to the community. The Volunteers Influencing Inmate Outcomes System (VIIOS) will utilize the FedRAMP-certified Salesforce Software-as-a-Service (SaaS) platform to enable BOP Reentry Affairs Coordinators (RAC) and Reentry Sector Chiefs (RSC) to track and manage institution needs for volunteers.

BOP staff will use the system to create online postings that detail the institution's needs for volunteers to the public. Prospective volunteers will be able to create profiles via a portal, view opportunities, and express interest in becoming a volunteer within the BOP by applying with relevant personal information. BOP has prepared a Privacy Impact Assessment for VIIOS because this system collects, maintains, and disseminates information in identifiable form about the prospective volunteers, as well as emergency contacts of the prospective volunteers, affiliated inmates, and BOP staff. The application information submitted by each prospective volunteer will be used by BOP staff to evaluate that prospective volunteer, initiate a background investigation, and track clearance status. The website will collect detailed web analytics about the general location of user traffic, the type of browser and operating system used to access the site, the date and time of access, the internet address of the website from which users linked directly to the site, and the pages visited and the information requested. This information is used to improve the performance of the website and leveraged to measure marketing efforts and improve future recruitment strategies. The information of individual website visitors is not identified/stored in the system or available to the system owners. The system uses Google Analytics to capture usage and system owners are displayed aggregated metrics on the platform.

Upon deployment, the volunteer recruitment system will transform volunteer management activities from a paper-based process to a digital one, including the status of the volunteer (approved/denied/pending and active/inactive), training management, visitation management and badge management.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

VIIOS will improve the realignment of volunteer recruitment and management activities with First Step Act (FSA) legislation goals and priorities. Needs for volunteer assistance at facilities and specific departments are digitally disseminated to the public to create awareness and grow interest. To submit applications, prospective volunteers are required to provide personal information, contact information, date of birth and place of birth information, current employer information, inmate affiliations, suitability questions and government-issued identification that is used to run background checks to ensure the safety of inmates and BOP personnel. Additional information including sponsoring organization and supplementary documents (e.g. letter of endorsement, letter of reference, professional certification) are requested to analyze the qualifications of prospective volunteers and finalize selection.

After completing an application, prospective volunteers can always navigate back to their submission through the website to view the information submitted and application status. BOP personnel reviewing the applications can also grant prospective volunteers the ability to update incorrect information if needed. Once a volunteer is accepted and onboarded, their information is maintained in VIIOS to track their eligibility for volunteer status, training requirements, visitation authorization, and badge access allocation.

The information regarding applicants and accepted volunteers can be retrieved by authorized BOP personnel with access to the system using the name of the applicant or volunteer and a unique auto-generated system identifier. The system uses "least privilege" methodology as access to information in VIIOS is limited to only the information necessary to process the request (e.g. access to volunteer information is limited to only the volunteer information necessary to process the particular request, and only to the authorized BOP staff at that location.) Approved DOJ contractors are involved with the design and development of the information system and will continue to provide maintenance and administrative services on the production environment after the information system is deployed.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	18 U.S.C. §§ 3621, 4042, 4082 and 5003 (state inmates), Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC felons); First Step Act (FSA) of 2018 (P.L. 115-391)
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, C, D	Full names and former names of applicants and volunteers. First and last names of emergency contacts, inmates, and BOP personnel.
Date of birth or age	X	C, D	Date of birth of applicants and volunteers.
Place of birth	X	C, D	Place of birth of applicants and volunteers.
Gender	X	C, D	Eye color, gender, hair color, height, and weight of applicants and volunteers.
Race, ethnicity, or citizenship	X	C, D	Race, ethnicity, and U.S. Citizenship of applicants and volunteers.
Religion			Although applicants or volunteers may provide religion-related information for various purposes, the prospective volunteer is never prompted for information on their religion on an application.
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	Social Security Number (full) of applicants and volunteers
Tax Identification Number (TIN)			
Driver's license	X	C, D	Driver License Number of applicants and volunteers.
Alien registration number	X	C, D	Alien Registration Number and Visa Number of applicants and volunteers.
Passport number	X	C, D	Foreign Passport Number of applicants and volunteers.
Mother's maiden name			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Vehicle identifiers			
Personal mailing address	X	C, D	Street, city, state, and zip code of applicants and volunteers.
Personal e-mail address	X	C, D	Email addresses of applicants and volunteers.
Personal phone number	X	C, D	Primary and secondary phone number of applicants and volunteers.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	C, D	Application information on volunteer applicants. Information elements collected are indicated in this table.
Education records			
Military status or other information			
Employment status, history, or similar information	X	C, D	Employment status, employer name, employer phone, employer street, employer city, employer state, and employer zip code of applicants and volunteers.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates	X	C, D	Professional certification of applicants and volunteers.
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **User passwords/codes**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **IP address**	X	A	System admin / audit data and User ID of authorized BOP personnel.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Date/time of access**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **Queries run**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **Content of files accessed/reviewed**	X	A	System admin / audit data and User ID of authorized BOP personnel.
- **Contents of files**	X	A	System admin / audit data and User ID of authorized BOP personnel.
Other (please list the type of info and describe as completely as possible):	X	C, D	Supplementary documents provided with application may include additional personal information regarding potential volunteers or other individuals. The website for prospective volunteers will capture audience, acquisition, and behavior metrics for web analytics.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other Federal Entities	

Government sources:					
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

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

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Direct log-in access is granted to approved BOP personnel such as RACs, RSCs, and Reentry Services Division (RSD) leadership. BOP personnel are limited to accessing the information from the areas or regions that they are approved for. Ad-hoc requests will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
				Reoccurring requests will be evaluated to determine need and minimum access to the system will be granted to satisfy the request.
DOJ Components	X			Information may be shared with other DOJ components in support of ad-hoc reporting requests for auditing or aggregated program metrics to measure success (e.g. volunteer registrations, application submissions). Ad-hoc reporting requests will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent.
Federal entities	X			Information may be shared with other Federal entities in support of ad-hoc reporting requests for auditing or aggregated program metrics to measure success. Ad-hoc reporting request will be sent to system owners, evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov

(a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

BOP has published two relevant System of Records Notices in the Federal Register:

DOJ's Inmate Central Records System, Justice/BOP-005, last published in full on May 6, 2019 (84 Fed. Reg. 19808), available at: https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf, and

Access Control Entry/Exit System, Justice/BOP-010, last published in full on April 8, 2002 (67 Fed. Reg. 16760). Available at: https://www.gpo.gov/fdsys/pkg/FR-2002-04-08/pdf/02-8424.pdf.

A Privacy Act (e)(3) notice will be provided to prospective volunteers on all pages of the application when populating and submitting information required for opportunities. A link to the BOP's privacy notice/policy is available on the footer of all pages for view by registered and prospective volunteers.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Prospective volunteers are provided notice through a Privacy Act Statement displayed by the system that: "Furnishing the requested information is voluntary, but failure to provide all or of part the information may result in lack of further consideration to provide services, clearance or access, or in the termination of your voluntary services."

Volunteers may, in the alternative, apply using the existing paper-based process. The existing paper-based process is addressed in the 2011 VCI PIA, available at https://www.bop.gov/foia/docs/vci.pdf. However, the paper-based process requests the same information from the prospective volunteer and includes the same notice regarding voluntary participation in the Privacy Act Statement as noted above.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act

procedures)? If no procedures exist, please explain why.

After completing an application, prospective volunteers can navigate to their submission through the website to view the information submitted and application status. BOP personnel reviewing the applications can also grant prospective volunteers the ability to update incorrect information if needed.

Alternatively, individuals may follow BOP protocols to receive or amend information collected or stored by BOP through a Privacy Act or FOIA request, which is outlined on the privacy policy page available to registered and prospective volunteers.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ATO is pending completion of this PIA. **If an ATO has not been completed, but is underway, provide status or expected completion date:** The ATO is pending the completion of this PIA. **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** N/A
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Thorough testing of security controls has been undertaken to ensure the proper monitoring and safeguarding of information.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The system captures an audit of user account modifications and system events that will be routinely reviewed by system administrators. Additional auditing of transactional data will be captured and maintained to align with records & information management requirements. A subset of approved internal users (e.g. employees, contractors) have been identified as system administrators to support organization-defined configuration, security, and access control.

X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: No additional system-specific privacy training.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Accounts are created for a subset of identified internal users (e.g. employees, contractors) which leverage single sign-on (SSO) and multi-factor authentication (MFA) using enterprise authentication services. Inbound requests to the internal application are restricted to monitor usage and leverage additional security controls from BOP. Role-based and permission-based policies define which records each user has access to with granular control using attribute-driven filters.

Approved internal users have been identified as system administrators to support organization-defined configuration, security, and access control. The account managers periodically review accounts to identify personnel that no longer need access in accordance with DOJ and federal requirements.[1] Account managers will add new users, remove existing users, or modify existing users. Automatic account management will be applied to inactivate accounts that have not logged into the system for a specified period of time. The system incorporates security controls to identify and restrict unsuccessful login attempts. Additional password complexity, reset duration, and reset reusage have been implemented to align with BOP standards.

The application is built using Salesforce, which uses industry best practices for data encryption at rest and in transit: Advanced Encryption Standard (AES) with 256-bit is used for data encryption at rest and Transfer Layer Security (TLS) is used for data encryption in transit.

Additional best practices are applied on session and login settings for users on the external-facing website, including policies on password expiration, reuse, and complexity, login attempts, and user lockouts, among other access and authentication protections.

6.3 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.)

[1] Details of the account audit process will be recorded in DOJ's Cyber Security Assessment and Management (CSAM) system.

The applicable records schedules for the system are detailed below.

GRS 2.2, Item 110
Volunteer service case files. Records documenting service performed without compensation by people not under a federal appointment. Includes both students as defined in 5 U.S.C. 3111 and nonstudents. Records include: volunteer agreements documenting position title, office title, duty location, days/hours on duty; parental approval forms; performance evaluations; training information; certificates of appreciation; correspondence documenting inclusive dates of service and total hours or days worked.

Information will be destroyed 4 years after a volunteer departs service; however, longer retention is authorized if required for business use. Automated batch jobs will run to evaluate the age of information and delete the data using hard (immediate) or soft (15-day temporary holding period) deletes. The retention periods are determined in accordance with BOP data storage/retention policy.

GRS 2.2, Item 120
Skill set records. Records detailing name, contact, and other information for people with specific skill sets, such as foreign languages, notaries, and sign language; used to assign work-related duties to employees and volunteers.

Information will be destroyed when the business use ceases. Automated batch jobs will run to evaluate the age of information and delete the data using hard (immediate) or soft (15 day temporary holding period) deletes. The retention periods are determined in accordance with BOP data storage/retention policy.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

DOJ's Inmate Central Records System, Justice/BOP-005, last published in full on May 6, 2019 (84 Fed. Reg. 19808). Available at: https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf.

Access Control Entry/Exit System, Justice/BOP-010, last published in full on April 8, 2002 (67 Fed. Reg. 16760). Available at: https://www.gpo.gov/fdsys/pkg/FR-2002-04-08/pdf/02-8424.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

a. Potential Risks Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish BOP's official duties is a potential threat to privacy arising from VIIOS. The unnecessary collection of data poses a risk of the loss of personal information to BOP volunteers, applicants, BOP staff, and inmates due to the sensitivity of the data involved, such as Social Security Numbers, Drivers' License numbers, and employment information. BOP mitigates this risk by implementing measures to limit the collection of data to that which is required to complete the authorized and necessary functions of VIIOS. These measures include creating certain defined data fields where required information can be inserted and evaluating each step, form, and field to determine need and minimize the amount of information collected.

There is also a potential privacy risk arising from collecting information of inadequate quality on each individual. To mitigate this, the VIIOS collects information directly from the prospective volunteer about whom the information pertains to the greatest extent practicable. The system only collects required information from a prospective volunteer after the individual voluntarily creates an account and expresses interest in providing volunteering services. The system displays a Privacy Act statement on all pages of the application when the prospective volunteer is populating and submitting information required for opportunities. A link to the BOP's privacy notice/policy is available on the footer of all pages for prospective volunteers which includes information on the following:

1. Information Collected
2. How Personal Information Is Used
3. Child Privacy
4. Cookie Usage
5. External Sites
6. Security

In order to mitigate the risk of unauthorized access or use, the collected information is safeguarded in accordance with BOP rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system.

b. Potential Risks related to the Use of Information

Potential threats to privacy arising from BOP's use of the information in VIIOS include the risk of unauthorized use of information, threats to the integrity of the information arising from unauthorized access or improper disposal of information. BOP mitigates the risk of

unauthorized access through the implementation of data access controls, ensuring information is provided only to those individuals who require access to perform their official duties.

Staff are annually trained on how to properly handle sensitive information to mitigate the risks arising from improper use or disposal of the information. The duration of time to retain information is determined when business use ceases in accordance with BOP data storage/retention policy. Additionally, in order to address the threats to the integrity of the data from unauthorized access, there are no outside users who are permitted access to the internal VIIOS system, including personnel from the larger DOJ community. Prospective volunteers will only have access to their own information through the website. When a BOP employee departs from the BOP or transitions to a new position, the BOP takes appropriate measures to deactivate the user access and accounts to VIIOS.

c. Potential Risks Related to the Dissemination of Information

There is a privacy risk to individuals arising from the potential disclosure of sensitive information to persons not authorized to receive it and unauthorized data modification and misuse. This risk is mitigated by enforcing access controls and encryption (as described above) and by providing auditing of user and system administration activities. Data transmission, both within and outside the system, is encrypted using the TLS protocol. Data within the system is used and shared only when required by the agency's mission.

Information required by law or DOJ policy to be shared for auditing of the VIIOS or for measuring success of the BOP volunteer program may be shared on a case-by-case basis with other DOJ components and Federal agencies. For example, under the First Step Act of 2018, the Attorney General is tasked to report to Congress on an annual basis the numbers of volunteer working in BOP facilities, per facility. Other types of dissemination request are evaluated to determine need, and the minimum information required to satisfy the request will be exported/sent. Any data shared with other DOJ components required by law or DOJ policy for reporting purposes will be aggregated and will have personal identifiers removed to make individual identification extremely difficult. These restrictions help address the risk of disclosure of information to unauthorized individuals both inside and outside BOP.