Federal Bureau of Prisons

Privacy Impact Assessment
for the
Compassionate Release/Reduction-in-Sentence Tracking System (RIS)

Issued by:
Michael Rogers
RIM Chief / SCOP

Approved by: Victoria Garcia
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: July 15, 2026

(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.)

The Federal Bureau of Prisons (FBOP) is responsible for the custody and care of federal inmates (as well as District of Columbia inmates committed to its care under the National Capital Revitalization Act). In accordance with federal law, inmates, or members of the public on behalf of the inmate, may make a request for the FBOP to file a motion on the inmate's behalf with their sentencing court to obtain a reduction in their sentence. The FBOP developed the Compassionate Release/Reduction-in-Sentence Tracking System (RIS) to replace a prior system and improve tracking of compassionate release/reduction-in-sentence requests and related documentation. RIS tracks the status of the request from its initiation through the disposition phase.

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.

RIS is used to track compassionate release/reduction-in-sentence requests received from federal inmates, as permitted by federal law and regulations. FBOP policy permits members of the public the ability to make a compassionate release/reduction-in-sentence request on behalf of an individual inmate. Federal inmate information is collected, maintained, and used to process the requests. Federal inmates and certain members of the public submit their requests to the inmate's institution's Unit Team via a hard copy letter, email, or on a FBOP Inmate Request to Staff form (Form BP-A0148). The FBOP's applicable program statement on compassionate releases/reductions in sentences, including instructions for submitting requests, is available on the FBOP's public website at https://www.bop.gov/policy/progstat/5050_050_EN.pdf.

When an inmate or member of the public submits a request, the FBOP Unit Team employees initiate the review process and manually enter and upload the information into RIS. RIS is interconnected with CICLOPS, which allows authorized FBOP employees (Unit Team) to view and manually insert the inmate's name, register number, and facility information maintained in CICLOPS into RIS to begin the request submission. RIS then provides a tracking number for that unique request, which allows FBOP to track the adjudication and routing of the request.

Once the request is entered into RIS and receives a tracking number, the inmate's Unit Team conducts a review of the request. During the review process, authorized employees upload relevant documents into the system, which gives the Unit Teams and later reviewers, such as Wardens, OGC, and FBOP

leadership, access to required and relevant request information. Relevant documents may include, but are not limited to, inmate criminal records, relevant medical and health information, FBOP disciplinary records, Pre-Sentence Investigation Reports (PSRs) from the U.S. Probation Office, United States Attorney's Office (USAO), or a law enforcement agency.

At minimum, the request for an inmate's compassionate release/reduction-in-sentence must include the following information in order for the request to be processed: (1) the extraordinary or compelling circumstances that are the basis for the request, and (2) proposed release plans. For all RIS requests, the following factors are considered in the review process: Nature and circumstances of the inmate's offense, criminal history, comments from victims, unresolved detainers, supervised release violations, institutional adjustment, disciplinary infractions, personal history derived from the PSR, length of sentence and amount of time served (this factor is considered with respect to proximity to release date or Residential Reentry Center (RRC) or home confinement date), inmate's current age, inmate's age at the time of offense and sentencing, inmate's release plans (employment, medical, financial), and whether release would minimize the severity of the offense.

Most of the review process is internal to FBOP. However, for requests reviewed by the FBOP Director, FBOP is required to solicit the opinion of the prosecuting United States Attorney's Office. Additionally, in some cases, the Office of the Deputy Attorney General may conduct a review. These non-FBOP entities do not have access to RIS. Instead, FBOP forwards the requests via email to the entities on a case-by-case basis.

After FBOP determined the inmate has met the RIS criteria and the Warden is considering whether to refer the case for further review, victims of those inmate requesting compassionate release/reduction-in-sentence are invited to provide any comments they would like to be considered as part of that process. When identifying whether there are victims to notify, the Unit Team staff will check CICLOPS to determine whether the inmate is subject to victim notifications. If CICLOPS indicates there is a required victim notification, the Unit Team reviewer then logs into VNS, enters the using the inmate's name and register number, and generates a notification letter that is sent to the identified victim(s) via VNS. Only victims who are identified in the VNS and consent to notification are notified by FBOP that there is a pending inmate compassionate release/reduction-in-sentence request under consideration. RIS includes a "notes" tab in which reviewers can leave notes or comments, which would include victim responses.

Once the FBOP internal reviews are complete and approved by the Director, the FBOP OGC then makes a motion to the relevant sentencing court under 18 U.S.C. §§ 4205(g) or 3582(c)(1)(A).

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. § 3582(c)(1)(A): A sentencing court, on motion of the Director of the Bureau of Prisons, may reduce the term of imprisonment of an inmate sentenced under the Comprehensive Crime Control Act of 1984; 18 U.S.C. § 4205(g): A sentencing court, on motion of the Bureau of Prisons, may make

		an inmate with a minimum term sentence immediately eligible for parole by reducing the minimum term of the sentence to time served; D.C. Code § 24-403.04: Motions for compassionate release for individuals convicted of felony offenses.
	Executive Order	
X	Federal Regulation	28 CFR §§ 571.60-64 (Compassionate Release Rules); 572.40 (stating that 18 U.S.C. § 4205(g) was repealed in 1987 but still applies to inmates whose offenses occurred before that data, while later offenses are governed by 18 U.S.C. § 3582(c)(1)(A)).
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	FBOP Program Statement 5050.50- Compassionate Release/Reduction in Sentence: Procedures for Implementation of 18 U.S.C. §§ 3582 and 4205(g).

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 and D	First and last name of FBOP employees and requestor (members of the public and convicted federal inmates).
Date of birth or age	X	C and D	Date of birth of convicted federal inmate.
Place of birth	X	C and D	POB of inmate.
Sex	X	C and D	Sex of inmate
Race, ethnicity or citizenship	X	C and D	Race of inmate
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C	SSN of inmates are included in uploaded Pre-Sentence Investigation Reports (PSRs) (U.S. Citizens only).
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C and D	Alien registration numbers may be included in uploaded PSRs.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	Mailing address of the requesting members of the public, if provided.
Personal e-mail address	X	C and D	E-mail address of the requesting members of the public, if provided.
Personal phone number	X	C and D	Phone number of the requesting members of the public, if provided.
Medical records number			

(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
Medical notes or other medical or health information	X	C and D	Federal inmate medical summary, medical condition, and life expectancy.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C and D	Federal inmate discipline and progress reports, and release plans.
Certificates			
Legal documents	X	C and D	Court documents from the inmate's relevant case file.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Federal inmate criminal records (relevant offense conviction history).
Juvenile criminal records information	X	C and D	Inmate juvenile criminal records may be included in uploaded PSRs.
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	X	C and D	Victim comments in response to potential compassionate release/reduction-in-sentence of inmate
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**			

(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
- **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 User IDs of Authorized FBOP staff.
- **User passwords/codes**	X	A	FBOP staff User passwords.
- **IP address**			
- **Date/time of access**	X	A	Date/time of access of FBOP staff.
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			

(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
Other (please list the type of info and describe as completely as possible):	X	A, B, C and D	Federal Register numbers of convicted inmates are collected, stored, and accessed. Tracking numbers assigned to the request are linked to the inmate's federal register number and name. Due to the broad scope of what may be discussed in a request, including the details related to a request for compassionate release/reduction-in-sentence and post-release plans, it is possible more data elements in the PII Chart above are collected in RIS; however, the elements selected above indicate the foreseeable elements collected by RIS.

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	X	Hard copy: mail/fax	X	Online	
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			

Government sources:
Other (specify): RIS may include an individual's criminal history from a state, local, tribal, or foreign government entity via an uploaded PSR, not from the government entity itself.

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Members of the public include individuals who submit requests on behalf of the inmates and victims who provide responses to submitted requests.					

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	Authorized FBOP staff, primarily within the inmate's FBOP Unit Team, OGC, Health Services Division, Correctional Programs Division, and system administrators, have access to the system.
DOJ Components	X			Upon request, ordinarily in the context of RIS litigation, authorized FBOP staff share information such as an inmate's request, a warden's denial memorandum, or an OGC denial memorandum with the relevant USAO handling an inmate's criminal matter. Information is transmitted to USAOs using secure email or the Justice Enterprise File Sharing (JEFS) system.

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.**
Federal entities	X			Upon request, ordinarily in the context of RIS litigation, authorized FBOP staff share information such as an inmate's request, a warden's denial memorandum, or an OGC denial memorandum. Correspondence with the courts is typically through the USAOs, rather than directly from FBOP. Under 18 U.S.C. § 3582 (d)(3), the FBOP Director must submit to the House and Senate Judiciary Committees an annual report on requests for sentence reductions pursuant to subsection (c)(1)(A).
State, local, tribal gov't entities				
Public	X			Victims may be notified about the submission of a request. Victims are notified by FBOP request reviewers if the victim consents to notification via VNS.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Upon request, ordinarily in the context of RIS litigation, authorized FBOP staff share information such as an inmate's request, a warden's denial memorandum, or an OGC denial memorandum with the requesting court pursuant to the specific request. Correspondence with the courts is typically through the USAOs, rather than directly from FBOP. Additionally, on occasion, after a request denial, an inmate's attorney may complete a request for the denial information.
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.

General notice will be provided via published SORN, Justice/BOP-005, DOJ's Inmate Central Records System, 84 Fed. Reg. 19808 (May 6, 2019), available at https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf.

In some instances, FBOP is required to notify certain inmates of their right to submit a request for compassionate release/reduction-in-sentence. For instance, pursuant to the First Step Act, FBOP is required to provide notice and assist terminally ill or debilitated offenders.

Additionally, pursuant to FBOP Program Statement 5050.50, FBOP institutions are required to notify federal inmates of (i) a defendant's ability to request a sentence reduction pursuant to subsection (c)(1)(A); (ii) the procedures and timelines for initiating and resolving requests described in clause (i); and (iii) the right to appeal a denial of a request described in clause (i) after all administrative rights to appeal within the Bureau of Prisons have been exhausted.

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.

As mentioned above, FBOP provides inmates notice of their ability to submit requests, and in some instances, are required to assist with certain inmates. Based on this notice, an inmate provides implied consent when they submit material for FBOP's consideration of a request for compassionate release/reduction-in-sentence.

Victims who consent to notification via VNS, receive communication from FBOP that explains the inmate's request for compassionate release/reduction-in-sentence is under review and they are permitted to provide FBOP with comments regarding the inmate's request. The notification states in part, "If you wish to submit written comments for consideration, please send your comments to this institution. Your comments will be carefully reviewed and given full consideration during our review of the inmate's request. Your comments will be included in any subsequent recommendations made by our staff to the sentencing court." This statement informs victims that their response/comment is optional.

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.

Pursuant to 28 CFR Part 513, inmates are provided the opportunity to review their documents upon request. Inmates can request FBOP correct information by completing the *Request to Staff Member* form (Form BP-A0148) and submit it to their Unit Team staff and include any documentation they may have as to why the data needs to be corrected or amended. The inmate receives notification of these procedures (how to amend or correct information) during their initial incarceration at the Admission and Orientation program, which every inmate is required to attend at initial admission and every time they are transferred to another facility. Federal Bureau of Prisons, Program Statement 5290.14, "Admission and Orientation Program Statement" (Apr. 3, 2003).

The public, including victims who submit responses or formerly incarcerated persons, are advised of the opportunity and method to access and amend their information pursuant to the Privacy Act via applicable System of Records Notice(s) (see Section 7.2 below). Information concerning FBOP's FOIA processes, including how to submit a FOIA or Privacy Act request, can be found at bop.gov.

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):** BOPNet ATO, authorized on 12/08/2025, and expires 12/08/2028. **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **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:
	This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2

	rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: RIS maintains Criminal Incarceration information. If a loss of availability, integrity, or confidentiality regarding this information were to occur, the worst-case scenario would be that individuals may suffer from unauthorized access of criminal information, which may result in identity theft or reputation harm, and the FBOP may suffer an adverse effect on public and inmate confidence. Under NIST SP800-60 Volume 2, Rev 1, this information properly falls under Federal Correctional Activities, with default categorization of Moderate, and special factors listed that could result in higher or lower impact level. The special factors listed are: None. Based on the specific facts of this scenario, there are no mitigating or aggravating factors, special factors are not implicated because the information type categorizations held within RIS are sufficient, resulting in Moderate impact level.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** FBOP IT System Administrators, the Cybersecurity Office, and privacy employees and contractors manage and maintain compliance of configuration changes required for maintenance, vulnerability management, and all continuous monitoring aspects of the system. They also perform configuration changes to improve the RIS security posture when necessary. These activities include updating configuration baselines to remediate vulnerabilities, applying all security patches and editing of continuous monitoring profiles to increase auditing capabilities.
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:** RIS follows the Audit and Accountability (AU) controls by NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. The system tracks user account modifications and system events that will be reviewed by system administrators on a quarterly basis. Additional auditing of transactional data will be captured and maintained to align with records and information management requirements. A subset of approved internal users have been identified as system administrators to support organization-defined configuration, security, and access control. Auditing by the system administrator provides visibility into important security events via log files and suspicious activities, which are forwarded to FBOP Cybersecurity Office/IT for correlation, reporting, and archiving on a regular basis. Audit and accountability procedures are reviewed annually, and audit and accountability policies are reviewed every three years.
	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 training conducted.

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?

Access to the system and data is limited to those FBOP employees who have an appropriate security clearance and are authorized to review such information for their official duties. Such access is regularly reviewed by system administrators. User access is restricted to those staff who need to view and upload data, and user roles are defined to limit capability and reduce risk of authorized access, use, or disclosure of RIS information. System access is web-based using a unique userID and password. Access to the network requires two-factor authentication. All transmissions of data are encrypted using the Transport Layer Security (TLS) encryption protocol.

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.)

The applicable National Archives and Records Administration (NARA) Disposition Authority is N1-129-00-23: Compassionate Release Files: Temporary: Archive when 4 years old or when no longer needed for reference, whichever is later. Destroy 15 years after cutoff.

Once hardcopy request letters are uploaded into the RIS system, the uploaded electronic copy is considered the official record.

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).

Yes, information in the system can be retrieved by a personal identifier, namely the inmate register number or RIS case tracking number.

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:

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

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Unauthorized disclosure: There is a risk of unauthorized disclosure or access of RIS information. RIS mitigates this risk by implementing data access controls, ensuring information is provided only to those authorized FBOP individuals who require access to perform their official duties. FBOP also does not permit non-FBOP users with direct access to the RIS system, which includes other DOJ component personnel. When an FBOP employee departs from the FBOP or transitions to a new position, the FBOP takes appropriate measures to deactivate the user access and accounts to RIS. FBOP employees are annually trained on how to properly handle sensitive information. Further, information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access; requirements to keep technical equipment in restricted areas; and required use of proper passwords and user identification codes to access the system. User access to RIS information is also segregated by user's institution, limiting staff's ability to access inmate information unless the inmate is physically located/assigned to the local site.

   There is an additional privacy risk related to potential unauthorized disclosure of RIS information when information is shared with external entities. Some information in RIS is shared with external entities as outlined in Section 4.1. Sharing with external federal agencies is done on a case-by-case basis in accordance with established agreements. Technical safeguards to mitigate the risks associated with the transmission of RIS information includes encryption of encrypted transmission of RIS information, both within and outside RIS. Additionally, FBOP attempts to mitigate the risk of sharing an inmate's information with the wrong victim by using VNS, rather than other methods of generating communication to known victim(s). As part of processing the inmate's request at the inmate's institution, Unit Team staff will check CICLOPS to determine whether the inmate is subject to victim notifications. If CICLOPS indicates there is a required victim notification, the Unit Team reviewer then logs into VNS, enters the using the inmate's name and register number, and generates a notification letter that is sent to the identified victim(s) via VNS.

b. Unauthorized data modification and misuse: There is also a risk of 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.

Additionally, as mentioned earlier, FBOP employees also receive annual training on how to properly handle sensitive information and must adhere to Bureau rules and policy governing automated information systems security and access or risk disciplinary or criminal consequences.

c. Overcollection or Collection of Inaccurate Information: There is a risk of RIS collecting and maintaining more information than necessary to accomplish FBOP's official duties, as well as collecting and maintaining inaccurate information. FBOP mitigates these risks by only collecting information directly from the individual for whom the request pertains or a member of the public who sends in a request on behalf of an inmate, and only information that is required to complete the authorized and necessary functions of RIS. FBOP notifies inmates about what information is required to complete a RIS request in the program statement listed in Section 2.2. To further mitigate the risk of inaccurate information, FBOP employees processing requests are trained to only collect documentation that is needed to process the request in RIS-specific training.

d. Collection of Sensitive Information: RIS collects information that can cause reputational, emotional, financial, or physical harm if it were released in an unauthorized manner. For example, RIS collects and maintains information from victims of inmates requesting compassionate release/reduction-in-sentence, as well as inmate social security numbers, health information, and criminal information.

Victim information disclosed to an unauthorized individual can result in further emotional harm to the victim and make them susceptible to threats or intimidation from the inmate or individuals close to the inmate. FBOP safeguards victim information by only inputting the victim response into RIS. While some victim responses may include victim PII, FBOP does not add victim PII in addition to the responses and the responses are subject to FBOP procedures for inmates requesting access to records, as well as the Privacy Act and FOIA. These processes allow for redaction of victim information, if any, prior to release. FBOP also exempts victim responses from inmate disclosures, as noted in FBOP inmate record access procedures and pursuant to Privacy Act law enforcement exemptions, 28 C.F.R. § 16.97 (exemptions claimed pursuant to 5 U.S.C. § 552a(j). This prevents inmates from knowing the victim issued a response/comment relating to their request, and helps prevent future harms, intimidation, or harassment against the victim for submitting a response/comment. Additionally, similar to the other information included in RIS, victim responses, and any victim PII contained therein, is subject to the same cybersecurity and access protections that apply to RIS.

Inmate information disclosed to unauthorized individuals can result in identity theft and reputational harm. FBOP mitigates this harm, as mentioned in subsection 8.a. above.