U.S. Department of Justice

Office of Justice Programs

Bureau of Justice Statistics

Washington, DC 20531

BUREAU OF JUSTICE STATISTICS
DATA PROTECTION GUIDELINES

Contents

Overview

The Bureau of Justice Statistics (BJS) is a federal statistical agency[1] and the nation's primary source for

[1] The Office of Management and Budget (OMB) recognizes BJS as one of 13 principal federal statistical agencies that have statistical work as their principal mission. See, Fundamental Responsibilities of Recognized Statistical Agencies and Units, 88 Fed. Reg. 56708, 56710 (August 18, 2023)

criminal justice data.[2] BJS is a component of the Office of Justice Programs (OJP) in the U.S. Department of Justice (DOJ). BJS's mission is to collect, analyze, publish, and disseminate statistical information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. These data are critical to federal, state, and local policymakers in combating crime and ensuring that justice is both efficient and evenhanded.

The BJS Data Protection Guidelines, developed in coordination with OJP's Office of the General Counsel and Office of the Chief Information Officer, provide a summary of the many federal statutes, regulations, and other authorities that govern BJS.[3] The guidelines highlight BJS's requirements to: adhere to strict confidentiality requirements regarding data collected at BJS's direction; ensure that the collected data be used only for statistical purposes; commit to wide dissemination of BJS data for public benefit; and strive to maximize the utility, objectivity, and integrity of the information BJS disseminates and archives for public use.

Data Protections in Federal Statutes

As a federal statistical agency, BJS is generally required by law to ensure confidentiality and use the data it collects exclusively for statistical purposes. [34 U.S.C. §§ 10134 and 10231]. Pursuant to its statutory responsibilities, BJS must maintain the confidentiality of information identifiable to a private person (also called personally identifiable information, PII, or identifiable information).[4] Specifically, in accordance with BJS's authorizing statute, the Director of BJS "shall be responsible for the integrity of data and statistics and shall protect against improper or illegal use or disclosure."[5]

Further, under 34 U.S.C. § 10231(a), no officer or employee of the federal government, including BJS employees or BJS data collection agents,[6] may use or reveal any research or statistical information furnished in connection with a BJS data collection, including data identifiable to any specific private person, by any person for any purpose other than the purpose for which it was furnished.

Additionally, under § 10231, statistical information provided to BJS that is identifiable to a private person is immune from legal process, and may not, without the consent of the person furnishing such information, be admitted as evidence or be used for any purpose in any action, suit, or other judicial, legislative, or administrative proceedings. Any person violating these confidentiality provisions may be punished by a fine not to exceed $10,000 in addition to any other penalty imposed by law.

Further penalties for unlawfully revealing or disseminating BJS's statistical data are found in 18 U.S.C §

[2] For the purpose of this document, the terms "data" and "information" are used interchangeably.

[3] This document is intended to provide a general overview of the statutory, regulatory, and policy framework under which BJS employees and its data collection agents operate. Nothing herein is intended to, or does, create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal. Any specific questions regarding the application of these statutes, regulations, policies, and guidelines should be addressed in writing to BJS directly. The BJS Data Protection Guidelines will be reviewed and updated periodically to reflect changes to current or newly implemented statutes, regulations, and other authorities. The most current version will be available on the BJS website.

[4] Under BJS's confidentiality regulations, "information identifiable to a private person means information which either—(1) Is labelled by name or other personal identifiers, or (2) Can, by virtue of sample size or other factors, be reasonably interpreted as referring to a particular private person." 28 C.F.R. § 22.2(e).

[5] 34 U.S.C. § 10132(b).

[6] The term "data collection agent" refers to the entity (e.g., a private or nonprofit research organization or an institution of higher learning) that receives funding from BJS through a cooperative agreement, grant, contract, subaward, or subcontract to conduct statistical activities. Individuals that work under such an award are included in this definition. BJS data collection agents are subject to applicable federal laws, regulations, and other authorities that govern BJS.

1905. Such penalties include mandatory termination from employment, as well as a fine, term of imprisonment of not more than one year, or both.

Data Use Restrictions in Federal Statutes and Regulations

As a federal statistical agency, by law BJS may use the data it collects only for statistical or research purposes and is required to ensure confidentiality.[7] Title 34 U.S.C. § 10134, states that "[d]ata collected by the Bureau shall be used only for statistical or research purposes, and shall be gathered in a manner that precludes their use for law enforcement or any purpose relating to a private person[8] or public agency other than statistical or research purposes." The term "*statistical purpose*" means "the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups."[9] Statistical purposes exclude "any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent."[10]

BJS data collection agents working with identifiable information collected or maintained at BJS's direction are required to comply with all applicable confidentiality requirements of 34 U.S.C. § 10231, the privacy certification requirements of 28 C.F.R. § 22.23, the requirement to destroy identifiable data as set forth in 28 C.F.R. § 22.25, and other relevant authorities that govern BJS.

FOIA Requests and Federal Confidentiality Protections

BJS data collections also have protections under a broader federal statute that affects the confidentiality of information in the Privacy Act of 1974 and the Freedom of Information Act (FOIA), 5 U.S.C. § 552. Although FOIA is generally cited as establishing the public's right of access to federal records and information, there are nine established FOIA exemptions which permit executive branch agencies to withhold certain types of information from release. For example, one such exemption may allow BJS to withhold information when public release would reveal information accusing a person of a crime.[11] Another example may allow BJS to refuse to disclose information if the information sought would "disclose investigatory records compiled for law enforcement purposes, or if the disclosure might have similar implications."[12] BJS will maintain the confidentiality of all PII sought by a FOIA request unless specifically instructed to disclose under a court order.

Federal Regulations on the Confidentiality of Identifiable Data

Identifiable data collected by BJS and its data collection agents are maintained under the confidentiality provisions outlined in 28 C.F.R. Part 22.[13] Relevant provisions include −

[7] 34 U.S.C. §§ 10134, 10231.
[8] The term "*private person*" means "any individual (including an individual acting in his official capacity) and any private partnership, corporation, association, organization, or entity (or any combination thereof)." 34 U.S.C. § 10251(a)(27).
[9] Section V of the E-Government Act of 2002 is also known as the "Confidential Information Protection and Statistical Efficiency Act of 2002," (CIPSEA). *See*, 44 U.S.C. § 3501 note.
[10] *Id*. at 502(5)(A).
[11] 5 U.S.C. § 552b(b)(5).
[12] 5 U.S.C. § 552b(b)(7).
[13] While the confidentiality provisions of Part 22 discussed herein are extensive, these regulations do not apply to any records from which identifiable research or statistical information was originally obtained; or to any records which are designated under existing statutes as public; or to any information extracted from any records designated as public.

- Information identifiable to a private person may be used or revealed only for research or statistical purposes, or where prior consent is obtained from an individual.

- BJS will restrict the volume of PII collected, used, or retained to the minimum necessary.

- Identifiable information will be used or revealed only to BJS employees and data collection agents on a need-to-know basis, and only if the recipient is legally bound to use it solely for research or statistical purposes, and to take adequate administrative and physical precautions to ensure confidentiality.

- BJS data collection agents are required by federal law, as a condition of funding, to maintain the appropriate measures and controls to adequately safeguard the administrative and physical security of identifiable data, as applicable.

- Individuals, including data collection agents, with access to data on a need-to-know basis are advised in writing of the confidentiality requirements and must certify in writing to abide by these requirements.

- BJS will employ formal sanctions against anyone failing to comply with DOJ policies and procedures, in accordance with applicable laws and regulations.

Information System Security and Privacy Requirements

BJS/OJP maintains a robust IT security program in compliance with the DOJ Cybersecurity Program[14] and the DOJ IT Cybersecurity and Privacy Rules of Behavior (ROB) for General Users[15] to facilitate the privacy, security, confidentiality, integrity, and availability of BJS/OJP's computer systems, networks, and data in accordance with applicable federal and Department policies, procedures, and guidelines. BJS's data collection agents are similarly required to maintain the appropriate administrative, physical, and technical safeguards to protect identifiable data and ensure that information systems are adequately secured and protected against unauthorized disclosure.

Specifically, BJS and its data collection agents are required to, where applicable −

- Assess and secure information systems in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).[16]

- Adhere to *Federal Standards for Security Categorization of Federal Information and Information*

[14] The provisions of DOJ Order 0904, *Cybersecurity Program*, apply to all DOJ components, personnel, and IT systems used to process, store, or transmit Departmental information, as well as to contractors and other users of IT systems supporting the operations and assets of DOJ. The provisions discussed herein provide a summary of DOJ's information technology security requirements and policies.

[15] The DOJ IT Security ROB for General Users apply to all DOJ components, personnel, and contractors and pertain to the use, security, and acceptable level of risk for DOJ systems and applications. The provisions discussed herein provide an overview of DOJ's information technology security requirements and policies. For a more extensive description of specific DOJ policies, requirements, roles, and responsibilities, consult the DOJ IT Security ROB for General Users in full.

[16] Pub. L. No. 113-283

Systems (FIPS 199) National Institute of Standards and Technology (NIST) guidelines to categorize the sensitivity of all information collected or maintained on behalf of BJS.

- Once the system has been categorized, secure data in accordance with the Risk Management Framework specified in NIST SP 800-37 rev. 2, along with NIST SP 800-60 rev.1, Volumes I&II.

- Employ adequate controls outlined within NIST SP 800-53, Rev5 to ensure data are not comingled with any other dataset or product without the express written consent of BJS (applicable to BJS data collection agents).

- Limit access to identifiable data to only those individuals who must have such access, including requisite IT security administrators.
- Limit the use of identifiable data to only the purposes for which its use was approved.
- Complete data security and confidentiality trainings.

Technical controls

Technical control of BJS data is maintained through a system of firewalls and encryption. OJP employs an Intrusion Detection System at the perimeter of the network to supplement its defense-in-depth approach to security. BJS maintains data on a secure hard drive behind the DOJ firewall, and the data are encrypted to meet Federal Information Process Standard (FIPS) Publication 140-2 requirements. Access to this drive and its files require username and password verification. Access to individual files is restricted to BJS project staff and the requisite OJP IT security administrators.

The Cybersecurity Enhancement Act of 2015[17] requires the Department of Homeland Security (DHS) to provide cybersecurity protection for federal civilian agency information technology systems and to conduct cybersecurity screening of the Internet traffic going in and out of these systems to look for viruses, malware, and other cybersecurity threats.[18] In accordance with the Act's provisions, DHS conducts these cybersecurity screening activities solely to protect federal information and information systems from cybersecurity risks. To comply with the Act's requirements and to enhance cybersecurity protections, all information that is transmitted to and from OJP systems is screened for cybersecurity threats including data collected and maintained under BJS's authority.

Furthermore, OJP is required to periodically assess its security controls to determine their effectiveness, monitor and correct deficiencies, reduce or eliminate vulnerabilities in IT systems, and monitor IT system security controls.

Physical controls

All on-site, physical BJS data files are stored in a secure building in Washington, D.C., which is staffed by guards 24 hours a day, 7 days a week. Federal employees and contractors must pass through an electronic badge swipe to verify their identity, and non-federal visitors must be sponsored by DOJ employees, record information in a central logbook, and wear a visitor's badge. Onsite servers containing BJS data are stored in a locked room with access limited to OJP IT personnel only and require a badge swipe to enter. BJS limits its storage of physical media that contains PII. Paper surveys, CD-ROMS, or other physical media that contain PII reside in a locked office with limited key access to authorized individuals, and all data use in the room is logged. BJS digitizes and destroys physical media as soon as practical, consistent with federal requirements.

[17] Codified in relevant part at 6 U.S.C. §151.

Data Collection Agent requirements

BJS's data collection agents must employ similar administrative, physical, and technical controls to adequately secure their information systems from unauthorized disclosure and must maintain controls equivalent to FISMA-moderate level protection standards. OJP reserves the right to audit during the project period any information system used by BJS's data collection agents to collect, receive, handle, maintain, transfer, process, store, or disseminate data products that maintain data collected or stored under BJS's authority to assess compliance with federal laws and regulations related to data management and security.

Dissemination of Data

The BJS authorizing statute reads, in relevant part, that BJS is authorized to "provide information to the President, the Congress, the judiciary, state, tribal, and local governments, and the general public on justice statistics."[19] A robust dissemination program is essential to the execution of this statutory mandate. BJS uses its website for data dissemination, including public access to data releases of aggregate statistics in the form of updated time series, cross-tabulations of aggregated characteristics of respondents, analytic reports, briefs of key findings, and technical reports. Aggregated data are typically made available in spreadsheet format and through online tabulation tools.[20]

Microdata published under BJS's authority, and the related study documentation, are made available to researchers for statistical and research purposes at the University of Michigan's National Archive of Criminal Justice Data and the Census Bureau's Federal Statistical Research Data Center (FSRDC), to the extent practical and subject to strong confidentiality protections. The level and format of access depends on the type of data being requested.

BJS follows established information dissemination practices, including those outlined in OMB's *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies*[21] as well as those outlined in BJS's Data Quality Guidelines.

BJS also adheres to OMB's Statistical Policy Directive No. 4, *Release and Dissemination of Statistical Products Produced by Federal Statistical Agencies*, and the standards on dissemination of information products set forth in OMB's Statistical Policy Directive No. 2, *Standards and Guidelines for Statistical Surveys.*

Data Archiving Practices

Consistent with its statistical mission and subject to strong confidentiality protections, BJS makes its published microdata available for secondary analysis to support replication and encourage further research in the field of criminal justice.

BJS applies the necessary statistical techniques to mitigate disclosure risks and determines the appropriate access method to protect confidentiality. Microdata files are available as either public-use or restricted-use files. BJS protects respondent confidentiality in public-use and restricted-use files by applying the appropriate statistical disclosure limitation techniques to mitigate disclosure risk, such as removing, masking, blanking, or collapsing direct and indirect variable and records.

[19] 34 U.S.C. § 10132(c)(10).
[20] Some older publications that are not machine readable may only be available on the BJS website via scanned PDF files.
[21] 67 Fed. Reg. 8,452 (February 22, 2002).

Microdata files that do not include PII are available for public use and may be downloaded. Microdata files that require additional confidentiality protections are accessible to approved researchers in a restricted setting. BJS adheres to the requirement for Federal statistical agencies to use a uniform application process with standard review and approval criteria to accept and review applications for restricted data (confidential statistical data).[22]

Prospective users of BJS's restricted data must apply and be approved for access through the Standard Application Process (SAP).[23] Approved researchers must fulfill the following minimum requirements: use BJS restricted data only for statistical or research purposes; operate the required technical, administrative, and physical controls to protect the data; adhere to BJS's disclosure review and output rules; and comply with Federal regulations to protect human subjects.

BJS makes some restricted-use data available through the FSRDC network, which is comprised of secure enclaves managed by the Census Bureau. FSRDCs provide secure environments to protect confidentiality. Prospective FSRDC users of BJS's data must also apply and be approved through the SAP.[24]

For more information about the SAP, see M-23-04 *Establishment of Standard Application Process Requirements in Recognized Statistical Agencies and Units*.

Data Retention Practices

BJS and its award recipients follow federal regulations requiring the disposition of data containing identifiable information.[25] Where applicable, BJS complies with all federal government data destruction guidelines regarding the technical and physical wiping of data from servers and destruction of existing CD-ROMs or paper documents. BJS's data collection agents are required to adhere to applicable BJS data disposition requirements, which include destroying PII collected in conjunction with BJS-funded activities upon delivery of the data to BJS and project completion.

Incident Response Procedures

DOJ has established incident response plans and notification procedures in the event of an actual or suspected data breach or other security incident involving PII and/or loss of any devices containing these data. These procedures apply to all BJS employees and its data collection agents and all PII regardless of format (e.g., paper, electronic, etc.). The response and notification procedures follow the requirements set forth in applicable DOJ Orders, federal statutes, policies, regulations, and other authorities, including the Privacy Act of 1974, the E-Government Act of 2002, FISMA, and OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information.*

In the event of a real or suspected data security incident involving PII by BJS or one of its data collection agents, BJS shall follow applicable requirements and work with the appropriate DOJ officials to investigate, report, mitigate, and respond to an actual or suspected security incident. Specifically, BJS will:

---

[22] 44 U.S.C. § 3583.
[23] M-23-04 Establishment of Standard Application Process Requirements on Recognized Statistical Agencies and Units (December 8, 2022).
[24] For more information about BJS's archiving practices, see https://www.icpsr.umich.edu/web/pages/NACJD/index.html and https://www.census.gov/about/adrm/fsrdc.html.
[25] 28 C.F.R. § 22.25 and National Archives and Records Administration.

- Notify, within one hour of discovery, the appropriate DOJ officials and law enforcement agencies.

- Provide DOJ forensics and law enforcement personnel, including the DOJ Inspector General, access to media and devices required for investigation, as appropriate.

- Assist with digital forensic and other investigations on electronic devices and/or associated media, as required.

- Record the handling and transfer of media and devices to support forensic and other investigations Notify individuals potentially impacted by the incident.

In the event of an incident involving PII, BJS may consult with the appropriate DOJ officials to develop mitigation options and assess the need to provide additional measures of protection, including analyzing whether a particular data loss appears to be resulting in identify theft and providing credit monitoring services to those impacted by the data incident.

Additionally, to further assist investigative and remedial efforts, BJS may disclose a limited amount of PII to the appropriate agencies, entities, and persons to assist in DOJ's response efforts or to prevent, minimize, or remedy harm to impacted individuals when it suspects or has confirmed an incident involving PII collected or maintained under BJS's authority. BJS may also provide a limited amount of PII to another federal agency or federal entity to assist their response efforts.

Indemnification

Any person who unlawfully discloses PII collected or maintained under BJS's authority shall be in violation of, and subject to the penalties provided by the confidentiality and criminal statutes referenced in the *Data Protections in Federal Statutes* section.

BJS will not agree to insure, defend, or indemnify its data providers. BJS will, consistent with DOJ authorities and subject to DOJ authorization, cooperate with the other party in the investigation and resolution of administrative claims and/or litigation arising from conduct related to the provisions of the separate data use agreement.

BJS Statistical Standards and Practices

Among BJS's fundamental responsibilities as a statistical agency is its duty to protect the trust of individual respondents and data providers by ensuring the confidentiality and exclusive statistical use of their responses.[26] As the nation's premier source of reliable criminal justice data, BJS is committed to employing robust data security protocols and data stewardship practices to protect the privacy and confidentiality of the data collected and maintained under its authority.

To uphold public trust in the integrity of the data and ensure continued cooperation from data providers and

[26] See, also, C.F.R. Part 1321 *Fundamental Responsibilities of Recognized Statistical Agencies and Units*.

respondents, BJS adheres to a set of statistical principles and practices[27] that guide its mission to compile, analyze, and disseminate information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government.

These principles include maintaining −

- Principle 1: Relevance to policy issues and society
- Principle 2: Credibility among data users and stakeholders
- Principle 3: Trust among the public and data providers
- Principle 4: Independence from political and other undue external influence
- Principle 5: Continual improvement and innovation

In addition, BJS adheres to the following standards −

- A clearly defined and well-accepted mission
- Necessary authority to protect
- Commitment to quality and professional standards of practice
- Professional advancement of staff
- An active research program
- Strong internal and external evaluation processes for an agency's statistical programs
- Coordination and collaboration with other statistical agencies
- Respect for data providers and protection of their data
- Dissemination of data products that meet users' needs
- Openness about the sources and limitations of the data provided

BJS Data Quality Guidelines

BJS has implemented and published the BJS Data Quality Guidelines that govern all justice data that BJS produces and disseminates for the general public in accordance with the provisions of the DOJ Information Quality Guidelines and OMB government-wide guidance for information dissemination, including the Paperwork Reduction Act (44 U.S.C. § 3501 *et seq*.). The BJS Data Quality Guidelines apply to a wide variety of substantive information and dissemination activities and topics, including −

- Privacy and maintaining confidentiality of data

[27] The *BJS Statistical Principles and Practices* were informed by *Principles and Practices for a Federal Statistical Agency*, 7th edition, National Research Council (2021), issued by the National Research Council of the National Academy of Sciences, which has guided managerial and technical decisions made by national and international statistical agencies for decades.

- Initiating surveys, censuses, and other data collections
- Survey design and data collections
- Data transparency, analysis, and processing
- Content and verification of BJS data
- Dissemination.

The BJS Data Quality Guidelines were established to ensure and maximize the utility, objectivity, and integrity of the information BJS disseminates and to provide a framework to give persons an opportunity to seek and obtain correction of information maintained and disseminated by BJS that does not comply with these guidelines.

Contact

Contact AskBJS@usdoj.gov with questions. Include *BJS Data Protection Guidelines* in the subject line.

Issue Date: May 20, 2016
Updated: September 9, 2025