U.S. Department of Justice

Office of Justice Programs

Bureau of Justice Statistics

Washington, D.C. 20531

BUREAU OF JUSTICE STATISTICS
DATA PROTECTION GUIDELINES

OVERVIEW

The Bureau of Justice Statistics (BJS) is a federal statistical agency[1] and the nation's primary source for criminal justice data. 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[2] 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 comprehensive summary of the many federal statutes, regulations, and other authorities that govern BJS. [3] As discussed in greater detail below, the guidelines require BJS 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.

I. DATA PROTECTIONS IN FEDERAL STATUTES

Pursuant to its statutory responsibilities, BJS must maintain the confidentiality of all personally identifiable information it collects. Specifically, in accordance with BJS's authorizing statute, the

[1] As described in *Statistical Programs of the United States Government, Fiscal Year 2016*, the Office of Management and Budget (OMB) recognizes thirteen principal federal statistical agencies that have statistical work as their principal mission.

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

[3] This document provides a general overview of the statutory, regulatory, and policy framework under which the employees of the U.S. Department of Justice, Bureau of Justice Statistics and its data collection agents and contractors operate. As such, it does not constitute legal advice; therefore, any specific questions regarding the application of these statutes, regulations, policies, and guidelines should be addressed to BJS directly in writing. As applicable, the BJS Data Protection Guidelines will be updated to reflect changes to current or newly implemented statutes, regulations, and other authorities. The guidelines are available on the BJS website – http://www.bjs.gov/content/pub/pdf/BJS_Data_Protection_Guidelines.pdf.

Director of BJS "shall be responsible for the integrity of data and statistics and shall protect against improper or illegal use or disclosure." 42 U.S.C. § 3732(b).

Further, pursuant to 42 U.S.C. § 3789(g), no officer or employee of the federal Government, including BJS employees or BJS data collection agents and contractors, 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 obtained.

Additionally, under that statute, 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. Finally, 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.

Finally, there is a general federal statute that prohibits any federal employee from disclosing "any information coming to him in the course of his employment or official duties . . . which information concerns or relates to . . . confidential statistical data . . ." 18 U.S.C § 1905. Penalties for violating this law include mandatory termination from employment, as well as a fine, term of imprisonment of not more than one year, or both.

II. DATA USE RESTRICTIONS IN FEDERAL STATUTES AND REGULATIONS

BJS operates under a statute which specifically states that it may only use the data it collects for statistical or research purposes. Title 42 U.S.C. § 3735 (section 304 of the Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. No. 90-351)), 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[4] or public agency other than statistical or research purposes." The term "*statistical purpose*," as defined in Section 502(9)(A) of the E-Government Act of 2002 means "the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups." [5] Statistical purposes exclude "any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent." *Id*. at 502(5)(A).

All of BJS's data collection agents and contractors involved in any stage of the statistical analysis process (including, but not limited to, the collection, receipt, handling, maintenance, transfer, processing, storage, and dissemination of data) are covered under the same protections as BJS employees during the duration of their contract pursuant to 42 U.S.C. § 3735 (section 304 of the Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. No. 90-351), as amended).

---

[4] 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)." 42 U.S.C. § 3791(a)(27).

[5] 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.

All of BJS's data collection agents and contractors as described above are also required to comply with all confidentiality requirements of 42 U.S.C. § 3789(g), the privacy certification requirements of 28 C.F.R. § 22.23, and the requirement to destroy identifiable data as set forth in 26 C.F.R. § 22.25.

III. 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.[6] 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."[7]

IV. FEDERAL REGULATIONS ON THE CONFIDENTIALITY OF IDENTIFIABLE DATA

Data collected by BJS and BJS data collection agents and contractors are maintained under the confidentiality provisions outlined in 28 C.F.R. Part 22.[8] Relevant provisions include the following:

- Data 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;

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

- BJS data collection agents and contractors are required by federal law, as a condition of funding, to submit a Privacy Certificate that describes the precautions in place to adequately safeguard the administrative and physical security of identifiable data, as applicable; and

- Individuals, including BJS data collection agents and contractors, 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.

[6] 5 U.S.C. § 552b(b)(5).
[7] 5 U.S.C. § 552b(b)(7).
[8] 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.

V. INFORMATION SYSTEM SECURITY AND PRIVACY REQUIREMENTS

BJS/OJP maintains a robust IT security program in compliance with the DOJ Cybersecurity Program[9] and the DOJ IT Security Rules of Behavior (ROB) for General Users[10] 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 data collection agents and contractors 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 BJS data collection agents and contractors are required to, where applicable:

- Assess and secure information systems in accordance with the Federal Information Security Modernization Act (FISMA) (Pub. L. No. 107-347), which appears as Title III of the E-Government Act of 2002 (Pub. L. No. 107-347);

- Adhere to 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. 1;

- Employ adequate controls to ensure data are not comingled with any other dataset or product without the express written consent of BJS (applicable to BJS contractors and data collection agents);

- Reduce the volume of personally identifiable information collected, used, or retained to the minimum necessary;

- Limit access to identifiable data to only those individuals who must have such access;

- Limit use of identifiable data to only the purposes for which it was approved;

[9] 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.

[10] 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, see the DOJ IT Security ROB for General Users in full.

- Log all computer-readable data extracts from databases holding sensitive information and ensure each extract including sensitive data has been erased within 90 days, or its use is still required;

- Ensure all contracts involving the processing and storage of personally identifiable information comply with DOJ policies on remote access and security incident reporting; and

- Employ formal sanctions for anyone failing to comply with DOJ policy and procedures, in accordance with applicable laws and regulations.

All on-site BJS data are stored in a secure building in Washington, D.C. which houses only OJP (including BJS) and is staffed by armed 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, pass through a metal detector, record information in a central log book, and wear a visitor's badge. Onsite servers containing BJS data are stored in a locked room with access limited only to OJP IT personnel, and require a badge swipe to enter. Data stored on CD-ROMs reside in a locked office with limited key access to authorized individuals, and all data use in this room is logged.

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 the BJS statisticians that work on the project, their direct supervisors, and the requisite OJP IT security administrators. All DOJ employees and BJS data collection agents and contractors are required to complete annual Computer Security Awareness Training and OJP information technology administrators are required to also complete annual training on security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, and procedures related to the security of DOJ and BJS/OJP IT systems and data, including digital and paper.

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.

BJS data collection agents and contractors must employ similar administrative, physical, and technical controls to adequately secure their FISMA-defined information systems from unauthorized disclosure. OJP also reserves the right to audit during the project period any FISMA-defined information system used by BJS data collection agents or contractors to collect, receive, handle, maintain, transfer, process, store, or disseminate data products in support of the project to assess compliance with federal laws and regulations related to data management and security.

The Cybersecurity Enhancement Act of 2015 (codified in relevant part at 6 U.S.C. § 151) required 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. DHS has implemented this requirement by instituting procedures such that, if a potentially malicious malware signature were found, the Internet packets that contain the malware signature would be further inspected, pursuant to any required legal process, to identify and mitigate the cybersecurity threat. 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 increase the protection of information from cybersecurity threats, OJP facilitates, through the DOJ Trusted Internet Connection and DHS's EINSTEIN 3A system, the inspection of all information transmitted to and from OJP systems including, but not limited to, respondent data collected and maintained by BJS.

VI. 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."[11] 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. All reports produced by BJS since 1994 are available electronically. Aggregated data are typically made available in spreadsheet format and through online tabulation tools.

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*[12] 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 standards on dissemination of information products set forth in OMB's *Standards and Guidelines for Statistical Surveys.*

VII. DATA DESTRUCTION PRACTICES

BJS and its data collection agents and contractors follow federal regulations requiring the destruction of data containing identifiable information.[13] 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 data collection agents and contractors are required to return or completely destroy any identifiable data collected on behalf of BJS upon delivery of the data to BJS and project completion.

[11] 42 U.S.C. § 3732(c)(10).
[12] 67 Fed. Reg. 8,452 (February 22, 2002).
[13] 28 C.F.R. § 22.25.

VIII. DATA ARCHIVAL PRACTICES

To support the facilitation of and encourage research in the field of criminal justice, BJS archives data at the National Archive of Criminal Justice Data (NACJD). To protect respondent confidentiality, BJS strips all direct identifiers prior to sending data to NACJD. NACJD takes additional precautions to mitigate compromising the confidentiality of data, including conducting a disclosure review to determine the appropriate level of security that should be applied to the data. In addition to the NACJD disclosure review, BJS may also request to suppress additional variables due to the sensitive nature of the data and/or to further protect confidentiality, if appropriate. Data that do not contain personally identifiable information are available for public access download. Prior to public release, NACJD routinely checks all data collections for conditions that could violate the confidentiality of data. NACJD protects respondent confidentiality by removing, masking, blanking, or collapsing direct or indirect variables within public-use versions of the dataset.

NACJD applies stringent security to restricted data where some risk of respondents' identity disclosure remains (e.g., variables used in conjunction with one another or linking to other data files) and provides four access options for these types of data: restricted access; physical data enclave; online analysis; virtual data enclave.[14] Prospective users of such data must follow NACJD's application and approval processes, including the submission of a research proposal and additional measures as required such as IRB approval or waiver, information about users of the data, a restricted data use agreement, and a data security plan. Additionally, users of data in the physical enclave must travel to the University of Michigan to analyze data on a NACJD computer in a secure room without internet and printer capabilities, and output is screened to ensure results are aggregated to a level that prevents individual identification.

BJS datasets stored at OJP and archived at the NACJD are periodically audited to determine if their security profiles have changed and protections need to be updated based on changes in policy, updates to OJP systems, or the availability of other linked data.

IX. INCIDENT RESPONSE PROCEDURES

DOJ has established notification procedures and incident response plans in the event of an actual or suspected data breach involving known loss of sensitive data and/or loss of any devices containing these data. These procedures apply to all BJS employees and BJS data collection agents and contractors, and all personally identifiable information regardless of format (e.g., paper, electronic, etc.).

In the event of a real or suspected data breach by BJS or a BJS data collection agent or contractor, BJS would be required to:

[14] The NACJD website provides specific details about its processes and requirements related to receiving and handling restricted data, including types of access and application requirements.

- Notify, within one hour of discovery, the Justice Security Operations Center (JSOC) and appropriate DOJ officials.[15] The JSOC would then report confirmed incidents within one hour to the United States Computer Emergency Readiness Team (US-CERT);

- Provide DOJ forensics and law enforcement personnel, including the U.S. 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; and

- Record the handling and transfer of media and devices to support forensic and other investigations.

In addition to establishing internal and external notification processes, the DOJ incident response procedures outline steps that DOJ or its contractors can take to mitigate the potential risk from loss of personally identifiable information and actions individuals can routinely take to mitigate their risk. In the event of a data breach by BJS involving personally identifiable information, BJS may consult with the DOJ Core Management Team in developing appropriate mitigation options, including assessing the need to provide two additional measures of protection: a data breach analysis to determine whether a particular data loss appears to be resulting in identify theft; and the provision of credit monitoring services to those impacted by the data breach.

The DOJ incident response procedures follow the requirements set forth in DOJ Order 0904, *Cybersecurity Program*, DOJ Order 2880.1C, *Information Resources Management Program*, DOJ Order 0900.00.01, *Incident Response Procedures for Data Breaches*; and OMB Memorandum M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* These procedures supplement the security and privacy requirements contained in the DOJ Security Program Operating Manual; the DOJ Computer System Incident Response Plan; the Privacy Act of 1974, and DOJ Order 3011.1A, *Compliance with the Privacy Requirements of the Privacy Act, the E-Government Act and the FISMA.*

X. BJS STATISTICAL STANDARDS AND PRACTICES

Among BJS's fundamental responsibilities as a statistical agency is its duty to protect the trust of information providers by ensuring the confidentiality and exclusive statistical use of their responses.[16] As the nation's premier source of reliable crime and 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.

[15] BJS data collection agents and contractors would be required to notify BJS within one hour of any security incidents that impact the FISMA-defined information systems that are used to collect, receive, handle, maintain, transfer, process, store, or disseminate data products in support of the project, including data files, reports, or working papers.

[16] See, also, OMB M-15-03 *Statistical Policy Directive No. 1: Fundamental Responsibilities of Federal Statistical Agencies and Recognized Statistical Units.*

To uphold public trust in the integrity of the data and ensure continued cooperation from data providers, BJS adheres to a set of statistical principles and practices[17] 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, including the:

- Commitment to quality and professional standards of practice;
- Timely and wide dissemination of data;
- Transparency about the sources of data and their limitations;
- Coordination and cooperation with other statistical agencies;
- Cooperation with data users; and
- Fair treatment of individuals, businesses, and institutions providing the data.

XI. 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. § 35). 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;
- Initiating surveys, censuses, and other data collections;
- Survey design and data collections;
- Data transparency, analysis, and processing;
- Content and verification of BJS data; and
- 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 under

[17] The *BJS Statistical Principles and Practices*) were informed by *Principles and Practices for a Federal Statistical Agency*, 5th edition, National Research Council (2013), 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.

which BJS will provide persons an opportunity to seek and obtain correction of information maintained and disseminated by BJS that does not comply with these guidelines.

Issue Date: May 20, 2016
Updated: February 6, 2017