

Month 202X



Electronic Data Extract Guide

Courts

Prepared by

Cynthia G. Lee

National Center for State Courts

300 Newport Ave

Williamsburg, VA 23185

OMB Control Number: ##### Expiration Date: #####

Contents

Section	Page
1. National Pretrial Reporting Program Overview	1-1
2. Data Preparation Instructions	2-1
2.1 Identifying Eligible Cases.....	2-1
2.2 File Structure.....	2-2
2.3 File Format.....	2-2
2.4 Supporting Documentation.....	2-2
3. Data Submission Instructions	3-3
3.1 Will the data be secure and kept confidential?.....	3-4
3.1.1 Data Transmission.....	3-4
3.1.2 Data Storage and Access.....	3-4
3.1.3 Data Publication.....	3-5
3.2 When is the submission due?.....	3-5
3.3 What if I am unable to provide all the requested data?.....	3-5
3.4 What happens after we submit the data?.....	3-5
3.5 Whom do I contact if I have questions?.....	3-6
Appendix	
Appendix A: Requested Data Elements, Definitions, and Formats	1

1. National Pretrial Reporting Program Overview

The goal of the Bureau of Justice Statistics' (BJS) National Pretrial Reporting Program (NPRP) is to collect information on persons charged with felony cases in state courts, and to collect contextual data on those persons from case filing to case disposition and sentencing. The NPRP will collect case-level information on pretrial release and detention, financial and other conditions associated with pretrial release, and any failures to appear, technical violations, or new arrests that occur during pretrial release.

The project will be completed in several phases by RTI International, with support from project partners the National Center for State Courts (NCSC), the National Association of Pretrial Services Agencies (NAPSA), Applied Research Services (ARS), and Pragmatica, Inc. The first phase collected information from states and counties about the systems that may collect and store these data. Such systems included courts, local jails, and pretrial services agencies. Data capacity surveys were conducted with each agency in the largest 200 counties in the U.S. The surveys allowed RTI and BJS to identify the data providers, understand their systems capabilities, and identify variables that potentially could be used to link the data across agencies.

The remaining phases involve a staged data collection from the 75 largest counties, and a sample of 50 of the remaining 125 counties. RTI and BJS have developed a sampling plan to maximize responsiveness and data representativeness and minimize respondent burden and project costs.

2. Data Preparation Instructions

This section outlines how to prepare and submit your NPRP data extract submission.

2.1 Identifying Eligible Cases

Courts. Your submission should define a case as all charges involved in a single incident filed into your system in calendar year 2019. At least one of the charges must be a felony offense. If a case may include multiple defendants involved in a single incident, please note this in your documentation and contact the NPRP staff listed in Section 3.5. If your case management system defines a case in some other way, please contact the NPRP personnel listed in Section 3.5.

2.2 File Structure

BJS is interested in a person-case and following that person-case from arrest and booking into jail, through pretrial processing to court case outcomes. This is an individual- and case-

level data collection. You can provide data in any format that is convenient for you, but we ask that you please provide supporting documentation, if available.

2.3 File Format

There is no required format for the data you submit; use whatever is most convenient for you. All file formats will be accepted. Some common file formats include:

- Text files (fixed width, delimited)
- Excel or .csv files
- Access database extracts
- SQL server database
- Data analysis software files (e.g., SAS, STATA, SPSS, or R data files)

The suggested coding classifications and value labels were developed to be as consistent as possible with the National Open Court Data Standards (NODS) and are provided in **Appendix A**. You are not asked to recode or manipulate your data prior to submission. If you have questions about any of the data elements requested, please contact the persons listed on the cover of this guide. We recognize that systems vary in terms of the ability to store, extract, and share data, and we are prepared to assist you.

Data from your jurisdiction will ultimately be combined with data from up to 75 other counties to gain a robust perspective on pretrial case processing in the U.S. During the data standardization process, RTI and NCSC may be in contact with jurisdiction personnel to request clarification on data fields and meanings to ensure that all submitted data are processed correctly.

2.4 Supporting Documentation

If possible, we ask that you provide supporting documentation with your submission. Specifically, we request:

- Date range of the data (e.g., 01/01/2019 through 12/31/2019)
- Date that the data extract was pulled
- Data point of contact (POC) (i.e., name, organization, address, telephone, and email address)
- File format of the data extract
- Known data limitations or quality issues
 - o Missing data:
 - System-missing (requested data element is not available in the system)

-
- Unit-missing (requested data element is available, but mostly blank or missing)
 - o Other common data issues include
 - Misspellings
 - Redundancy or duplication (e.g., two date fields for one event)
 - Data formatting information
 - o Data dictionaries, including variable/column names, variable description, expected variable values
 - o Any known discrepancies in the names of data elements in **Appendix A** and how your system labels the data elements

3. Data Submission Instructions

RTI will create a private, password-protected user account for each Data Point of Contact (Data POC) to upload data to Amazon Web Services (AWS) Simple Storage Service (S3). This AWS S3 storage location will only be accessible from designated network subnets. The Data POC will need to provide their subnet range or specific IP address from which they will be accessing AWS S3 from so the access control rules may be updated to grant access to the Data POC from their network. A free and easy way to discover your IP address is to go to <https://www.iplocation.net/> Once data access has been set up, the Data POC will log into their private account to transfer the requested data to a secure central data storage system on AWS S3.

Data security note: All data are encrypted in transit to AWS and at rest within AWS (SSL in transit and AES 256-encryption at rest), complying with the FIPS 140-2 standard. The secure AWS S3 repository will hold all raw data files received from the courts, jails, and pretrial services agencies until they are processed, linked, de-identified, and subsequently deleted by RTI data analysts. RTI controls access to the data storage system; all access to data resources will be logged, and the entire infrastructure will be reviewed and regularly scanned for vulnerabilities. The data storage system will be configured to deny public access by default, and we will use Amazon's Macie service to regularly scan and evaluate the security status of the storage. All RTI and NCSC staff granted access to data files (identified and deidentified files) will be required to sign a Staff Data Security Agreement. This pledge outlines staff responsibilities for protecting the confidentiality of all information identifiable to a private person that is collected during the project. The RTI Principal Investigator is responsible for maintaining up-to-date record of signed pledges.

3.1 Will the data be secure and kept confidential?

Consistent with its statutory obligations (34 U.S.C. § 10134), BJS only uses information collected under its authority for statistical or research purposes. Further, BJS is required by law to protect the confidentiality of all personally identifiable information (PII) it collects or acquires in conjunction with BJS-funded projects (34 U.S.C. § 10231), and must maintain the appropriate administrative, physical, and technical safeguards to protect the identifiable information against improper use or unauthorized disclosure. BJS will not use or reveal data identifiable to a private person, except as authorized under 28 CFR § 22.21 and § 22.22. The BJS Data Protection Guidelines summarize the federal laws, regulations, and other authorities that govern information acquired under BJS's authority, and are published on the BJS website: https://www.bjs.gov/content/pub/pdf/BJS_Data_Protection_Guidelines.pdf. RTI and NCSC are required to adhere to these same requirements as a condition of funding.

3.1.1 Data Transmission

RTI and NCSC project staff will receive data sets in a secure manner via an encrypted AWS GovCloud S3 server, appropriate for files with PII. RTI will create a private, password-protected user account that relies on an email address and IP address for each agency to upload data to the AWS S3 storage location. This AWS S3 storage location will only be accessible for the email and IP address granted access to the server. Any data set(s) electronically transmitted to BJS will be over the DOJ's Office of Justice Programs (OJP) secure transfer site.

3.1.2 Data Storage and Access

The secure AWS S3 repository will hold all raw data files received from the agencies until they are processed, linked, and subsequently deleted by RTI. Once received and linked with other available records, raw data files will be stripped of PII and replaced with an anonymous identifier. RTI will retain a PII-anonymous identifier crosswalk in case a revised file is submitted later. This file will be encrypted, password protected, and stored on a secure RTI server in the event the AWS S3 storage location is breached. Access to the S3 instance will be restricted to individuals with an identified business need. RTI controls access to the data storage system; all access to data resources will be logged, and the entire infrastructure will be reviewed and regularly scanned for vulnerabilities. PII is encrypted while in transit, and access to the data will be limited to those employees who have a need for such data and have signed a confidentiality pledge. The pledge includes an agreement to comply with all data security and human subjects' protection requirements.

3.1.3 Data Publication

BJS only publishes de-identified data at the aggregate level in its project findings, reports, data files, and other statistical products. BJS archives its published data and related data documentation (e.g., user guides) at the National Archive of Criminal Justice Data (NACJD), located at the University of Michigan. To the extent practical, BJS removes, masks, or collapses direct and indirect identifiers prior to sending data to NACJD to protect confidentiality. NACJD takes additional precautions to protect confidentiality, including conducting a comprehensive disclosure risk review to determine the appropriate level of security that should be applied to the data. For more information on data requiring additional security protections, please see:

<https://www.icpsr.umich.edu/icpsrweb/content/NACJD/restricted.html>.

We understand that your agency may have preexisting policies in place around data sharing, and we will work with your agency to meet any data transfer or agreement requirements you may have. While each of the identified data elements was selected to help fully understand the processing of case data, we recognize that not all data elements may be collected or readily available electronically for public use. Please notify us if you limit the amount or type of data you can release.

3.2 When is the submission due?

We ask that all participating agencies provide their data by ##/##/####. However, please reach out to the staff identified in Section 3.5 if you need additional time to submit your data.

3.3 What if I am unable to provide all the requested data?

We do not expect that any one organization has all of the data elements requested in Appendix A. Please provide those data elements that are available. If your agency does not collect any of the information in Appendix A, or if it would be too burdensome to provide the data, please contact the staff in section 3.5.

3.4 What happens after we submit the data?

RTI or NCSC will review the contents of the data files and conduct a series of checks to the data elements requested in the **Appendix A**. This should be completed within 2-4 weeks of submission. RTI or NCSC will then contact the Data POC to review and confirm the findings from the review. We may also have questions about variable values or labels, and will take all steps to understand your data submission.

3.5 Whom do I contact if I have questions?

Please reach out to Cynthia Lee (NCSC) at clee@ncsc.org or 757-259-1583 for questions or support in submitting your data to the AWS S3 server.

Appendix A: Requested Data Elements, Definitions, and Standard Formats

The following series of tables includes the data elements for the NPRP. The name of the variable and the description provided should help you to locate a similar data element in your data management systems. We are also including a standard format, which is how we expect to standardize the data you submit.

Please contact any of the NCSC personnel listed in 3.5 if you have any questions about the following data elements.

Table 1. Case-level data

Name	Definition	Standard Formats
Court case number	Unique identifier for case	
Associated case number	Unique identifier for this case at another court level. Used for purposes of linking limited jurisdiction and general jurisdiction cases.	
First name	The defendant's first name	Text, character, string
Middle name (if available)	The defendant's middle name	Text, character, string
Last name	The defendant's last name	Text, character, string
State ID number	The defendant's unique, fingerprint-supported state identification number	
FBI Number	The unique identification number given by the Federal Bureau of Investigation's Interstate Identification Index to each offender (if available)	
Other personal identifiers if SID and FBI number are not available	If SID and FBI number are not available, please provide any other unique identifier assigned to a person, such as a Social Security Number or Driver's License Number. Please describe in data documentation	

Name	Definition	Standard Formats
Other system identifiers assigned to a person	Include any other unique identifiers that specify the individual in your data system. For example, booking ID, inmate ID, or client ID. Please describe in data documentation.	
Date of birth or age	The defendant's date of birth. If not available, defendant's age (and please include age at what reference period in the documentation. For example, age at arrest, age at booking, age at filing)	mm/dd/yyyy
Sex	The defendant's biological sex/sex assigned at birth	Male, Female, Other, Unknown
Race	The defendant's race	(OMB race categories if available) White, Black or African American, Asian, Native Hawaiian or Other Pacific Islander, American Indian or Alaska Native, Other, Unknown.
Ethnicity	The defendant's ethnicity	Hispanic or Latino; Not Hispanic or Latino; Unknown. If race and ethnicity are stored in the same field, please contact one of the persons listed in Section 3.5
Date of offense	Date the alleged offense occurred	mm/dd/yyyy
Date of arrest	Date the individual was arrested for the offense	mm/dd/yyyy
Date court case filed	Date the case was filed in court	mm/dd/yyyy
Date of initial appearance	Date the defendant first appeared before a judicial officer after arrest. Typically, this initial appearance determines whether the defendant will be detained or released. Please include in data documentation what occurs at the first appearance after arrest	mm/dd/yyyy

Name	Definition	Standard Formats
Attorney type at initial appearance	Type of attorney representing the defendant at initial appearance, if any	Public defender, assigned/appointed counsel, private counsel, attorney of unknown type, no attorney
Date of arraignment	Date the defendant was arraigned. Arraignment typically includes advising defendant of charges against them, advising them of rights, and requesting the defendant to enter a preliminary plea. Please include in data documentation what occurs at the arraignment	mm/dd/yyyy
Number of FTAs	Number of times defendant failed to appear in this case	Integer
Any FTA	Did defendant ever fail to appear in this case?	Y/N
Disposition date	Final disposition date for the case as a whole	mm/dd/yyyy
Attorney type at disposition	Type of attorney representing the defendant at disposition, if any	Public defender, assigned/appointed counsel, private counsel, attorney of unknown type, no attorney
Attorney type at sentencing	Type of attorney representing the defendant at sentencing, if any	Public defender, assigned/appointed counsel, private counsel, attorney of unknown type, no attorney

Table 2. Charges—one record per charge, multiple records permitted per case

Name	Definition	Standard Formats
Court case number	Unique identifier for case	
Charge number	Identifier for charge within case (e.g., sequence number)	
Charge filing date	Date on which the charge was filed with the court	mm/dd/yyyy
Filing Charge Statute/Ordinance Number	The statute/ordinance number that defines the alleged behavior as an offense	Numeric
Filing NCIC Code	The NCIC code associated with the charge at filing	Text/Numeric
Filing Charge Description	Description of the offense at filing	Text
Filing Charge Degree	Charge class severity/degree at filing. For inclusion in the NPRP, at least one of the filed charges must be a felony	Felony, gross misdemeanor, misdemeanor, violation
Filing Charge Degree Detailed	The specific class severity or degree provided by statute for each charge against the defendant	Text
Filing Charge Modifiers	The specific type of mitigator or enhancer associated the filed charge	Attempt Conspiracy Solicitation Domestic Violence Use of a weapon Other
Disposition Charge Statute/Ordinance Number	The state statute/ordinance number that defines the alleged behavior as a criminal offense for each disposed charge	Statute or ordinance number
Disposition NCIC Code	The NCIC code associated with the charge at disposition	NCIC code
Disposition Charge Description	Description of the offense at disposition	Text
Disposition Charge Degree	Charge class severity/degree at disposition	Felony Gross misdemeanor Misdemeanor

Name	Definition	Standard Formats
		Violation
Disposition Charge Degree Detailed	The specific class severity or degree provided by statutory laws for each disposed charge	Text
Disposition Charge Modifiers	The specific type of mitigator or enhancer associated the disposed charge	Attempt Conspiracy Solicitation Domestic Violence Use of a weapon Other
Charge Disposition Date	Date when the charge received a judgment or disposition	Date
Charge Manner of Disposition	The manner in which the charge was disposed	Jury Trial Bench Trial Non-Trial
Charge Disposition	The judgment or disposition entered by the court for the charge	Bindover/Transfer Conviction at trial Guilty plea Acquittal Entry into a problem-solving court docket Diversion (not to a problem-solving court docket) Continued without a finding Dismissed/Nolle Prosequi Other
Charge Sentencing Date	Date when the charge received a sentence	Date

Table 3. Pretrial risk assessment—one record per assessment, multiple records permitted per case

Name	Definition	Standard Formats
Court case number	Unique identifier for case	
Date of pretrial risk assessment	Date the pretrial risk assessment was ordered or conducted	mm/dd/yyyy
Pretrial risk assessment instrument	Type of pretrial risk assessment administered.	
Risk assessment score	The risk assessment category assigned to the defendant. Include description of scores in the data documentation	

Table 4. Pretrial release determinations—one record per event, multiple records permitted per case

Name	Definition	Standard Formats
Court case number	Unique identifier for case	
Pretrial release determination type	Type of event	e.g., Initial appearance, Bail review, Revocation hearing
Date of pretrial release determination	Date of event	mm/dd/yyyy
Type of bond set	If bond was set, what type of bond was ordered	Cash bail, other financial bail, property bond
Bond amount information	If court set a financial bond, the amount ordered	Number
Bond posted	Was bond posted?	Y/N
Date bond posted	Date bond posted	mm/dd/yyyy
Type of detention ordered	Reason the court detained the defendant	No bond, preventive detention, other
Type of release ordered	Type of bond or release ordered, if applicable. Please detail in data documentation the types of release available in your jurisdiction	Personal recognizance/ROR, percentage/secured bond, unsecured bond, cash bond, property bond, other

Name	Definition	Standard Formats
Conditions of release	Conditions the defendant must follow when released pretrial	Release to supervising agency, electronic monitoring/house arrest, drug/alcohol testing, no contact order, program compliance, Ignition interlock, other
Attorney type at pretrial release determination	Type of attorney representing the defendant at this event, if any	Public defender, assigned/appointed counsel, private counsel, attorney of unknown type, no attorney
Bond modifications or revocations	If the defendant incurs a new arrest or violation of pretrial supervision and receives a revocation or modification of bond	
Date of bond modification or revocation	The date the bond is modified or revoked	mm/dd/yyyy

Table 5. Sentencing—one record per sentence type per case or charge; multiple records permitted per case/charge; indicate whether provided at case or charge level

Name	Definition	Standard Formats
Court case number	Unique identifier for case	
Charge number	Identifier for charge within case (e.g., sequence number), if sentence recorded at charge level	
Sentence Type	Type of sentence the defendant was mandated to serve.	death penalty life in prison state prison jail lifetime supervision extended supervision/split sentence probation fine/monetary penalty restitution community service time served other
Sentence Length	Length of sentence imposed by the court, by term. Indicate units (years, months, days, etc.) in data documentation.	Numeric
Sentence Conditions	Additional conditions imposed at sentencing.	Text
Concurrent/ Consecutive Sentence Flag	Flag to indicate the sentence is to be served concurrently or consecutively.	Yes/No
Time Served Credit Length	Length of time (specify units) spent in pretrial detention that was credited toward the sentence the defendant was mandated to serve.	Numeric
Monetary Penalty Type	A type or category of obligation, e.g., fee, fine, damages, court costs, special funds,	Fees Fines

Name	Definition	Standard Formats
	liquidated damages.	Damages Court costs Special Funds
Monetary Penalty Amount	Total dollar amount for each monetary penalty type	Currency
Restitution Amount	Dollar amount of restitution ordered	Currency
Alternative Fine Indicator	Was there a sanction or alternative to fine, such as community service	Yes/No