U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) National Data Exchange (N-DEx) System

Policy and Operating Manual

Version: 7.0
Document Date: November 22, 2022
N-DEx-DOC-09172-7.0

The *N-DEx Policy and Operating Manual* supersedes all pre-existing policy documentation and is the sole source for policy matters for the N-DEx System.

N-DEx System Policy and Operating Manual

Table of Contents

1.0 INTRODUCTION

1.1 Purpose

1.1.1 The National Data Exchange (N-DEx) Program Office Mission: To reduce crime and safeguard the American people by providing strategic information sharing solutions to the criminal justice and national security communities.

1.1.2 Scope of the N-DEx System policy: The N-DEx System Policy and Operating Manual applies to all entities accessing data through the N-DEx System, to include information residing in both the N-DEx System and in federated data sources. NDEx System information shall be used only for the purpose indicated by the Use Code and the Search Reason Requirement. When applicable, users must also comply with the Authorized Use Requirement (confirming the terms of N-DEx System information use). N-DEx System information shall be used only for the original purpose requested and a current record should be requested when needed for a subsequent authorized use.

1.1.3 The *N-DEx Policy and Operating Manual* integrates federal laws, presidential directives, Federal Bureau of Investigation (FBI) directives, and the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) decisions to provide criminal justice agencies (CJAs) and limited authorized federal non-criminal justice agencies (non-CJAs) with a minimum set of policy and procedural requirements for N-DEx System participation and to protect and safeguard criminal justice information. This minimum set of requirements ensures continuity of N-DEx System operational and information security.

1.1.4 The *N-DEx Policy and Operating Manual* may be used as the sole policy and operating manual for N-DEx System participating agencies. A participating agency may complement the *N-DEx Policy and Operating Manual* with agency specific policy and operating procedures, or the participating agency may develop their own stand-alone policy and operating manual; however, the *N-DEx Policy and Operating Manual* shall always be the minimum standard. Participating agencies may augment or increase the standards but shall not detract from the N-DEx Policy and Operating Standards.

1.1.5 The *N-DEx Policy and Operating Manual* applies to all entities with access to, or who operate in support of, N-DEx System services and information. This policy manual is subject to change as a result of federal laws, presidential directives, FBI directives, and CJIS APB decisions. The terms of any policy and procedural change preempt any existing inconsistency contained herein.

1.1.6 The *N-DEx Policy and Operating Manual* is an unrestricted document and can be shared without limitation.

1.2 Operational Framework

1.2.1 The N-DEx System is a system managed within the framework of the CJIS System of Services and identified within the CJIS Systems User Agreement.

1.2.2 Participating agencies and users must adhere to the *CJIS Security Policy*.

1.2.3 The N-DEx System stores vast amounts of criminal justice information which may be instantly retrieved by and/or furnished to any authorized agency.

1.2.4 The contents of the N-DEx System are restricted to documented criminal justice information obtained by criminal justice agencies in connection with their official duties administering criminal justice.

1.2.5 Within the context of the N-DEx System, federated access refers to the capability to access CJIS Systems of Services and non-CJIS criminal justice data sources, via web services. CJIS Systems are only available if the CJIS Systems Agency (CSA) authorizes this capability.

1.2.6 The N-DEx System will not contain criminal intelligence data, as defined by Title 28, Code of Federal Regulations (C.F.R.), Part 23.

1.2.7 The N-DEx System users who hold certifications under Title 28, C.F.R., Part 23 shall be permitted federated access to criminal intelligence information as the term is defined in Part 23.

1.2.8 Pursuant to Title 28 C.F.R., Part 20, and consistent with the *CJIS Security Policy*, access to the N-DEx System is restricted to "criminal justice agencies" performing the "administration of criminal justice." The N-DEx System may also be used to conduct background checks under the programs administered by the National Instant Criminal Background Check System (NICS) and the CJIS Division Bioterrorism Risk Assessment Group (BRAG).

1.2.9 The N-DEx System is the national enhanced pointer and data discovery system for Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES), and Controlled Unclassified Information (CUI) class criminal justice data.

1.2.10 The N-DEx System is a fee free, secure, nationwide, computerized information sharing system established to fill an identified gap in the CJIS System of Services.

1.2.11 The N-DEx Program is a cooperative endeavor of federal, state, local, and tribal law enforcement/criminal justice entities, in which each entity is participating under its own legal status, jurisdiction, and authorities. All N-DEx System operations will be based upon the legal status, jurisdiction, and authorities of individual participants.

The N-DEx System is not intended, and shall not be deemed, to have any independent legal status.

1.2.12 Agencies shall participate in the N-DEx System in accordance with their own individual legal status, jurisdiction, restrictions, and authorities.

1.2.13 Participating agencies contribute information to the N-DEx System with an express promise of confidentiality.

1.2.14 N-DEx System participants shall contribute or allow access to information via the N-DEx System, and agree to permit the access, dissemination, and use of such information by other parties, pursuant to the provisions of this policy. The record owning agency has the sole responsibility and accountability for ensuring it is not constrained from permitting this access by any laws, regulations, policies, or procedures.

1.2.15 The N-DEx System was not created pursuant to a single federal statute; rather, the N-DEx System is the FBI's response to the criminal justice community's request to answer the challenge of information sharing.

1.2.16 All inquiries regarding the N-DEx System should be addressed to the FBI, CJIS Division, via e-mail: ndex@leo.gov; via telephone: 888-334-4536; or via mail: Attention: N-DEx Program Office, Module D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306-0153.

1.3 Data Use

1.3.1 The N-DEx System shall be used according to the policies in this document, which apply to information residing in both the N-DEx System and in federated data sources. However, when the federated data source is a CJIS Systems of Service (SOS), such as NCIC, III, and NGI, the N-DEx System authorized use and verification policy does not apply. Rather, federated data source users must comply with all applicable policies governing the other system (i.e., the CJIS SOS). N-DEx System participating agencies that allow access to a CJIS SOS, through the N-DEx System, shall have procedures that require its users to comply with both N-DEx System policies (e.g., proper completion of the Use Code and Reason Field) and those of the CJIS SOS (e.g., procedures to confirm "hits" and to place a "locate" on an NCIC record).

1.3.2 An N-DEx System result indicates criminal justice information may exist.

1.3.3 N-DEx System Access: The N-DEx System contains criminal justice information obtained by CJAs in connection with their official duties administering criminal justice. N-DEx System access is restricted to CJAs performing the administration of criminal justice. Only the following agencies are authorized to access the N-DEx

System based on the agency type Originating Agency Identifier (ORI) value, as indicated by the ninth (9^{th}) character:

1.3.3.1 Law Enforcement Agencies (LEAs)

- LEAs possessing 9^{th} character ORIs of 0 - 9 (numeric values) e.g., police, sheriff, etc.

1.3.3.2 Criminal Justice Agencies

- Prosecuting Attorney's Offices – ORIs end in an "A." This includes District Attorney's Offices, Attorney General's Offices, etc.
- Pretrial service agencies and pretrial release agencies – ORIs end in a "B."
- Correctional Institutions - ORIs end in a "C." This includes jails, prisons, detention centers, etc.
- Nongovernmental railroad or campus police departments qualifying for access to the Interstate Identification Index (III) System – ORIs end in an "E."
- Probation and Parole Offices – ORIs end in a "G."
- INTERPOL – ORIs end in an "I." As a foreign CJA, INTERPOL shall be a Limited System Participant. Local, state, and tribal CJA data shall not be shareable with limited system participants.
- Courts and Magistrates Offices – ORIs end in a "J."
- Custodial facilities in medical or psychiatric institutions and some medical examiners' offices which are criminal justice in function – ORIs end in an "M."
- Regional dispatch centers which are CJAs or noncriminal justice governmental agencies performing criminal justice dispatching functions for criminal justice agencies – ORIs end in an "N."
- Federal, state, county, or local agencies classified as CJAs by statute, but do not fall into one of the aforementioned categories – ORIs end in a "Y."

1.3.4 Acceptable System Use: Personnel engaged in the following activities may be granted access by the CSA consistent with state laws:

1.3.4.1 Law enforcement investigations: to further investigations of criminal behavior based on prior identification of specific criminal activity by an agency with a statutory ability to perform arrest functions.

1.3.4.2 Pretrial release investigation: to obtain information about recently arrested defendants for use in deciding whether conditions are to be set for defendants' release prior to trial, monitor a defendant's compliance with his/her conditions of release during pretrial period, and identify offenses pending adjudication.

1.3.4.3 Intake investigation: to conduct prisoner classification and offender risk assessments to safely manage the correction population.

1.3.4.4 Correctional institution investigation: to identify and suppress criminal suspects and criminal enterprise organizations operating within correctional systems, prepare for the prosecution of crimes committed within a correctional institution, conduct criminal apprehension efforts of prison escapees, ensure inmates cannot continue their criminal activities through misuse of visitation or communication privileges, monitor outsource supervision and treatment progress, conduct offender travel permit investigations, prepare for prisoner transfer, and conduct pre-release investigation to determine reentry requirements and facilitate release notification.

1.3.4.5 Pre-sentence investigation: to identify the risk of re-offense, flight, community, officer and victim safety, identify law enforcement contact not resulting in arrest, identify offenses pending adjudication, and ensure illicit income is not used for bail, bond, or criminal defense.

1.3.4.6 Supervision investigation: to identify incident information (i.e. personal conduct, contact with LEAs, offenses, gang affiliations, known associates, employment, etc.) constituting a violation of release or supervision conditions, prepare and investigate interstate transfer of adult offenders, facilitate concurrent supervision, conduct risk and needs assessments, facilitate apprehension of absconders, and identify offenses pending adjudication.

1.3.4.7 Criminal justice employment background checks: to obtain information regarding an applicant’s fitness to serve as an employee within a CJA.

1.3.4.8 Data administration/management: to perform administrative role responsibilities and conduct searches of record owner contributed data as a part of internal review by a record owner. Responses for this purpose may not be disseminated for any other reason and are limited to that agency’s portion of N-DEx System contributed records.

1.3.4.9 Training: to educate users on the policies, services, and capabilities of the N-DEx System, utilizing authentic criminal justice information submitted to the N-DEx System by CJAs. Training is considered an acceptable use of the N-DEx System, provided it does not include curiosity searches, browsing, or self-queries.

1.3.4.10 Federal Security Clearances, Suitability and Fitness for Federal Employment and Credentialing, and Related Federal Matters background checks conducted by federal executive agencies in accordance with Executive Order 13488, as amended by Executive Order 13764.

1.3.4.11 NICS-related checks: to obtain information when conducting a NICS-related background check.

1.3.4.12 BRAG Assessments: to allow CJIS BRAG to conduct Security Risk Assessments on individuals to possess, use, or transport select biological agents and toxins.

1.3.5 N-DEx System Access Requirements: A user shall adhere to the following access requirements:

1.3.5.1 The user must be assigned to a valid ORI.

1.3.5.2 The user must have a user account via a CJIS Division recognized identity provider.

1.3.5.3 The user must have a national fingerprint-based check (within 30 days of assignment.)

1.3.5.4 The user must have a state of residency fingerprint-based check (within 30 days of assignment.)

1.3.5.5 The user must complete Security Awareness Training (within six months of assignment and biennially, thereafter.)

1.3.5.6 Access requirements may also include any state-required certifications, if applicable. However, it is the responsibility of the user and N-DEx Agency Coordinator (NAC) to ensure any additional state-imposed access requirements for the N-DEx System are met. See policy 1.6.4 for additional NAC duties.

1.3.6 User Identifier Requirement: A user shall provide the following user identifiers prior to accessing the N-DEx System:

1.3.6.1 Identity Provider ID: unique identifier indicating the system utilized to access the N-DEx System.

1.3.6.2 User ID: unique username assigned by the user's identity provider for authentication and identification.

1.3.6.3 Last Name: last name or family name of the user.

1.3.6.4 First Name: first name of the user.

1.3.6.5 Employer ORI: unique identifier assigned to the user's assigned agency. ORIs must be a CJIS NCIC assigned ORI.

1.3.7 Use Code Requirement: The FBI's CJIS Division is required to maintain an audit trail of each search request and returned result of N-DEx System data. Therefore, every N-DEx System search request must include a Use Code identifying why the search was performed.

The following Use Codes are considered acceptable when searching the N-DEx System:

1.3.7.1 Administrative Use Code "A:" Must be used when the N-DEx System is utilized by a record-owning agency or submitter/aggregator to retrieve and display N-DEx System contributed records in association with performing the agency's data administration or management duty. Responses for this purpose shall not be disseminated for any other reason and are limited to the record-owning agency portion of N-DEx System records.

1.3.7.2 Criminal Justice Use Code "C:" Must be used when the N-DEx System is utilized for official duties in connection with the administration of criminal justice, as the term is defined in 28 CFR § 20.3 (2011).

1.3.7.3 Criminal Justice Employment Use Code "J:" Must be used when the N-DEx System is utilized to conduct criminal justice employment background checks.

In order to use the N-DEx System to conduct criminal justice employment background checks, the agency must adhere to the following notice and consent, redress, and audit requirements:

- Notice and Consent: The agency must provide notice to the applicant and the applicant must provide a signed consent. At a minimum, one of the following or substantially similar statements must appear on an agency's Notice and Consent form to an applicant, examples of which are provided below:

    - General Statement: The (agency's name)'s acquisition, retention, and sharing of information related to your employment application is generally authorized under (state

and federal citations.) The purpose for requesting this information is to conduct a complete background investigation pertaining to your fitness to serve as a (employee type.) This background investigation may include inquiries pertaining to your employment, education, medical history, credit history, criminal history, and any information relevant to your character and reputation. By signing this form, you are acknowledging you have received notice and have provided consent for (agency's name) to use this information to conduct such a background investigation, which may include the searching of (the N-DEx System) (criminal justice databases) (private databases) (public databases.)

- Specific N-DEx System statement: I authorize any employee or representative of (agency's name) to search the N-DEx System to obtain information regarding my qualifications and fitness to serve as a (employee type.) I understand the N-DEx System is an electronic repository of information from federal, state, local, tribal, and regional criminal justice entities. This national information sharing system permits users to search and analyze data from the entire criminal justice cycle, including crime incident and investigation reports; arrest, booking, and incarceration reports; and probation and parole information. This release is executed with full knowledge, understanding, and consent that any information discovered in the N-DEx System may be used for the official purpose of conducting a complete employment background investigation. I also understand any information found in the N-DEx System will not be disclosed to any other person or agency unless authorized and consistent with applicable law. I release (agency's name) from any liability or damage which may result from the use of information obtained from the N-DEx System.

- Redress: The agency must provide applicants with an opportunity to challenge or correct records if employment is denied based on information obtained from the N-DEx System.

  - If employment is denied solely due to information obtained from the N-DEx System, and the applicant challenges the accuracy or completeness of those records, the denying agency shall provide the applicant with the contact information of the agency owning the information underlying the decision to deny. After receiving a written request from the applicant challenging the accuracy or completeness of the record used to deny employment, the record-owning agency shall then review the relevant information and advise the applicant in writing whether it has confirmed the

accuracy or completeness of its records, or whether the records will be corrected. If the applicant does not receive a response from the record-owning agency within 30 days from the date of the applicant's written request, the applicant may contact the FBI CJIS Division N-DEx Program Office, 1000 Custer Hollow Rd, Clarksburg, WV 26306. The FBI shall forward the challenge to the record-owning agency for verification or correction. The record-owning agency shall then review the relevant information and advise the applicant in writing whether it has verified its records or whether the records will be corrected. Agencies should inform applicants of their responsibility to provide any corrected information to the denying agency which may assist the record owning agency in its research on behalf of the applicant.

- Audit: The agency must comply with certain procedural and documentation requirements.

    - All use of the N-DEx System for criminal justice employment background investigations shall require Use Code "J." Agencies which contribute records to the N-DEx System shall be permitted and enabled to reject Use Code "J" requests. When the N-DEx System is searched as part of a criminal justice employment background investigation, the fact the search was conducted must be documented in the applicant's file. If information accessed through the N-DEx System is viewed and used during the criminal justice employment background investigation, the agency must document in the applicant's file: (1) the requesting agency received advanced authorization for the use of the information for employment purposes from the record-owning agency, and (2) the requesting agency has confirmed the accuracy of the information with the record-owning agency.

    - Agencies are expected to comply with the above requirements in addition to the existing N-DEx System policy requirements (e.g. training, information sharing, data quality, system security) and all applicable laws and regulations. These additional requirements mitigate the privacy risks of using the N-DEx System to conduct criminal justice employment background checks and ensure such use is implemented in a lawful and proper manner.

1.3.7.4 Federal Fitness/Suitability Use Code "S:" Must be used when the N-DEx System is utilized by qualifying federal agencies to conduct vetting for federal security clearances, suitability and fitness for federal employment and credentialing, and related federal matters. CSOs will designate users approved for the Use Code "S" capability from the qualifying federal

agencies, as defined by Executive Order 13488 as amended by Executive Order 13764.

In order to use the N-DEx System to vet individuals for federal security clearances, suitability and fitness for federal employment and credentialing, and related federal matters, the agency must adhere to the following notice and consent, redress, and audit requirements:

- Notice and Consent: The agency must provide notice to the applicant and the applicant must provide a signed consent. At a minimum, one of the following or substantially similar statements must appear on an agency's Notice and Consent form to an applicant, examples of which are provided below:

    - General Statement: The (agency's name)'s acquisition, retention, and sharing of information related to your application is generally authorized under (federal citations.) The purpose for requesting this information is to conduct a complete background check investigation pertaining to your fitness to serve as a (employee type.) This background investigation may include inquiries pertaining to your (employment) (education) (medical history) (credit history) (criminal history) and any information relevant to your character and reputation. By signing this form, you are acknowledging you have received notice and have provided consent for (agency's name) to use this information to conduct such a background investigation, which may include the searching of the (N-DEx System) (criminal justice databases) (private databases) (public databases.)

    - Specific N-DEx System statement: I authorize any employee or representative of (agency's name) to search the N-DEx System to obtain information regarding my qualifications and fitness to serve as a (employee type.) I understand the N-DEx System is an electronic repository of information from federal, state, local, tribal, and regional criminal justice entities. This national information sharing system permits users to search and analyze data from the entire criminal justice cycle, including crime incident and investigation reports; arrest, booking, and incarceration reports; and probation and parole information. This release is executed with full knowledge, understanding, and consent that any information discovered in the N-DEx System may be used for the official purpose of conducting a complete background investigation. I also understand any information found in the N-DEx System will not be disclosed to any other person or agency unless authorized and consistent with applicable law. I release

(agency's name) from any liability or damage which may result from the use of information obtained from the N-DEx System.

- Redress: The agency must provide applicants with an opportunity to challenge and/or correct records if federal security clearances, suitability and fitness for federal employment and credentialing, and related federal matters are denied based on information obtained from the N-DEx System.

    - If federal security clearances, suitability and fitness for federal employment and credentialing, and related federal matters are denied solely due to information obtained from the N-DEx System, and the applicant challenges the accuracy or completeness of those records, the denying agency shall provide the applicant with the contact information of the agency owning the information underlying the decision to deny. After receiving a written request from the applicant challenging the accuracy or completeness of the record used to deny the federal security clearance, suitability and fitness for federal employment and credentialing, and related federal matters, the record-owning agency shall then review the relevant information and advise the applicant in writing whether it has confirmed the accuracy or completeness of its records, or whether the records will be corrected. If the applicant does not receive a response from the record-owning agency within 30 days from the date of the applicant's written request, the applicant may contact the FBI CJIS Division N-DEx Program Office, 1000 Custer Hollow Rd., Clarksburg, WV 26306. The FBI shall forward the challenge to the record-owning agency for verification or correction. The record-owning agency shall then review the relevant information and advise the applicant in writing whether it has verified its records or whether the records will be corrected. Agencies should inform applicants of their responsibility to provide any corrected information to the denying agency which may assist the record-owning agency in its research on behalf of the applicant.

- Audit: The agency must comply with certain procedural and documentation requirements.

    - All use of the N-DEx System for federal security clearances, suitability and fitness for federal employment and credentialing, and related federal matters, shall require Use Code "S." Agencies which contribute records to the N-DEx System shall be permitted and enabled to reject Use Code "S" requests. When the N-DEx System is searched as part of a federal security clearance, suitability and fitness for federal employment and credentialing,

and related federal matter check, the fact the search was conducted must be documented in the applicant's file. If information accessed through the N-DEx System is viewed and used during the federal security clearance, suitability and fitness for federal employment and credentialing, and related federal matter check, the agency must document in the applicant's file: (1) the requesting agency received advanced authorization for the use of the information for federal agency vetting purposes from the record-owning agency and (2) the requesting agency has confirmed the accuracy of the information with the record-owning agency.

- Agencies are expected to comply with the above requirements in addition to the existing N-DEx System policy requirements (e.g. training, information sharing, data quality, system security) and all applicable laws and regulations. These additional requirements mitigate the privacy risks of using the N-DEx System to conduct vetting for federal security clearances, suitability and fitness for federal employment and credentialing, and related federal matters and ensure such use is implemented in a lawful and proper manner.

1.3.7.5 NICS-related checks Use Code "F:" Must be used when the N-DEx System is utilized to conduct NICS-related background checks.

The NICS-related checks must be made in accordance with the Brady Handgun Violence Prevention Act of 1993 (Brady Act). In addition, the N-DEx System shall purge all Use Code "F" search criteria in adherence with the Consolidated Appropriations Bill, H.R. 2673, as required by the NICS operating procedures and policies.

The Brady Act required the U.S. Attorney General to establish the NICS for Federal Firearm Licensees (FFLs) to contact for information to be supplied immediately as to whether the transfer of a firearm to an unlicensed person would violate Section 922 (g) or (n) of Title 18, United States Code (U.S.C.) or state law. In addition, NICS background checks may be conducted for the following purposes:

- Pursuant to Title 28, Code of Federal Regulations (C.F.R.), Section 25.6 (j)(1), "the NICS may provide information to federal, state, local, or tribal criminal justice agencies in connection with the issuance of a firearm-related or explosives-related permit or license."

- Title 28 C.F.R. §25.6 (j)(2) "permits the NICS to respond to inquiries by the Bureau of Alcohol, Tobacco, Firearms, and Explosives [ATF] in connection with a civil or criminal law enforcement activity relating to the Gun Control Act [of 1968] or the National Firearms Act."

- Title 28 C.F.R. §25.6 (j)(3) "for the disposing of firearms in the possession of federal, state, local, or tribal criminal justice agencies."

1.3.7.6 BRAG Use Code "B:" Must be used when the N-DEx System is utilized to conduct Security Risk Assessments on individuals to possess, use, or transport select biological agents and toxins, per Public Health and Bioterrorism Preparedness and Response Act of 2002 (The Bioterrorism Act) Public Law (PL) 107-188.

1.3.7.7 Redress procedures for Use Code "B" Security Risk Assessments are set forth in 42 U.S.C. § 262a and 42 CFR 73.20. Redress procedures for NICS-related checks are set forth in 28 CFR 25.10.

1.3.8 Search Reason Requirement: While the Use Code provides some lead information, it only provides a minimal audit trail. Therefore, all N-DEx System users are required to provide the reason for every search request. This will ensure N-DEx System searches are conducted for authorized uses and Use Codes are correctly applied. The Search Reason shall include information such as, but not limited to, incident number, arrest transaction number, booking number, project name, routine activity description, and if applicable, the individual recipient or agency the search was made "on behalf of," etc., to assist the user in accounting for appropriate system use for each transaction. III System searches, via the N-DEx System, shall clearly identify the individual recipient or agency the search was made "on behalf of." The identification shall take the form of a unique identifier which shall remain unique to the individual requester and to the secondary recipient throughout the minimum one-year retention period.

1.3.9 Authorized Use and Verification Requirement: N-DEx System information may be used and shared, without restrictions imposed by the record-owning agency, provided both of the following conditions are met:

- The recipient(s) of shared information resides within the record-requesting agency or within another authorized agency, with which a primary information exchange agreement exists; and
- The information will not be used for the following actions: inclusion of the information in an official case file; use in the preparation of judicial processes such as affidavits, warrants, or subpoenas; use in an adverse eligibility or suitability determination when retrieving information under Use Codes J, F, B or S; or dissemination to another authorized entity not part of the releasing agency's primary information exchange agreement (otherwise known as secondary dissemination).

Any sharing or use of N-DEx System data not meeting the above conditions requires the N-DEx System user to verify the information with the record-owning agency for completeness, timeliness, accuracy, relevancy, and any use restrictions on the data prior to actionable use or secondary dissemination of the data.

1.3.10 Immediate use of N-DEx System information can be made without the verification from the record-owning agency if there is actual or potential threat of criminal activity or terrorism requiring swift action to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect, or destruction of evidence. The record-owning agency shall be immediately notified of any use made as a result of above circumstances.

1.3.11 Participating record-owning agencies are encouraged to consider how they may wish to account for verification requests in a complete and timely manner, including the maintenance of accurate POC information on agency records. While the N-DEx System does not systematically support nor require a log to be maintained, agencies are encouraged to consider how verification requests may be documented within their own organization.

1.3.12 Information returned from the N-DEx System, regardless of whether it originally resided in the N-DEx System or in a federated data source, must be identified to the user as being received from the N-DEx System.

1.4 Responsibility for Records

1.4.1 Record-owning agencies which make available records in the N-DEx System are responsible for their timeliness, accuracy, completeness, and providing point-of-contact (POC) information. For further explanation of timeliness, accuracy, and completeness, see section 2.5, Maintaining the Integrity of N-DEx System Records.

1.4.2 Each record-owning agency controls how and with whom their data is shared, thus retaining responsibility, control, and ownership.

1.4.3 Agency-Configurable Data Sharing Controls: All data is presumed sharable. The record-owning agency may restrict data access in accordance with the laws, regulations, or policies which govern dissemination and privacy for their jurisdictions. Restricted data access requires the submission of relevant authorizing laws, regulations, or policies to the N-DEx Program Office. The N-DEx System enables data sharing at the following data item (i.e. reports) dissemination criteria values:

1.4.3.1 Green: Data is viewable.

1.4.3.2 Yellow: Data consists of record ID and record-owning agency POC information. To obtain access, contact the record-owning agency.

1.4.3.3 Red: Data is not viewable.

1.4.3.4 Record-owning agencies shall have the ability to configure sharing policy based on agency, agency type, or select data characteristics to create exception groups for their data.

1.4.4 Pursuant to Executive Order 12958 as amended, *Classified National Security Information*, the N-DEx System is designated as an unclassified system. Record-owning agencies shall ensure data contributed to and/or exchanged by the N-DEx System is unclassified and free of classified national security information. Information contributed to the N-DEx System resides in FBI controlled space, containing SBU and CUI from contributing agencies with established formal agreements.

1.4.5 All participating agencies, whether contributing information to the N-DEx System or federating to the N-DEx System, shall access the N-DEx System via secure internet connections (as defined by the *CJIS Security Policy*) or via the FBI's CJIS Wide Area Network.

1.4.6 The FBI CJIS Division, as manager of the N-DEx System, helps maintain the integrity of the system through:

1.4.6.1 Automatic computer checks which reject records with common types of errors in data.

1.4.6.2 Pre-data ingestion analysis and data inspection.

1.4.6.3 On-going manual quality control checks by FBI personnel.

1.4.6.4 Automated tool support, e.g., conformance testing assistance, for construction of data submissions.

1.4.6.5 System generated error reports for viewing by the record-owning Source Data Administrator (SDA) and CSA.

1.4.6.6 Monitoring and automated logging of all successful and unsuccessful logon attempts (where CJIS is the identity provider), file access, correlations, and transaction types, regardless of access means.

1.5 System Description

1.5.1 Full system participants are federal, state, local, and tribal CJA's throughout the U.S., District of Columbia, and U.S. territories.

1.5.2 Limited system participants are foreign CJAs. State, local, and tribal CJA data shall not be shareable with limited system participants, i.e. foreign CJAs.

1.5.2.1 The N-DEx System is the technical mechanism to bi-directionally share federal government unclassified criminal justice information with foreign partners, e.g., Australian Federal Police, New Zealand Police, and United Kingdom Serious Organized Crime Agency.

1.5.3 Data contributed to the N-DEx System must meet the criteria established for the particular type of record involved as identified in the N-DEx Information Exchange Package Documentation (IEPD).

1.5.4 In accordance with the *CJIS Security Policy*, criminal justice information shall refer to all FBI CJIS provided data necessary for CJAs to perform their missions. Such information shall consist of, but not be limited to biometric, identity history, biographic, property, and case/incident history data.

1.5.5 Data contributed and/or exchanged via the N-DEx System is criminal justice information, which contains Personally Identifiable Information (PII), e.g., names, social security numbers, etc., as well as, non-identifying descriptive information e.g., offense location, weapon involved, etc., and may contain criminal history record information as defined in Title 28, C.F.R., Part 20. The collection, storage, and dissemination of information shall comply with all applicable laws and regulations.

1.5.6 In accordance with the *CJIS Security Policy*, an information exchange agreement, i.e., a formal agreement specifying security controls must be signed before exchanging criminal justice information. Formal agreements may take the form of user agreements, management control agreements, CJIS security addendum, or any other document meeting the requirements articulated in the *CJIS Security Policy*.

1.6 Policy Management

1.6.1 The CJIS APB, established by Title 28, C.F.R., Part 20.35, recommends general policy to the FBI Director with respect to the philosophy, concept, and operational principles of the N-DEx System. In its deliberations, the APB places particular emphasis on system security; and rules, regulations, and procedures to maintain the integrity of CJIS System of Services and criminal justice information.

1.6.2 Detailed information on the operation of the APB process can be found within the *Bylaws for the Criminal Justice Information Services Advisory Policy Board and Working Groups*.

1.6.3 In accordance with the *CJIS Security Policy*, the CJIS Systems Officer (CSO) or designee shall ensure a Terminal Agency Coordinator (TAC) is designated within each agency which has devices accessing CJIS systems. The TAC serves as the POC for the CSO at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs with the local agency and oversees the agency's compliance with CJIS systems policies.

1.6.4 The CSO or designee shall ensure a NAC is designated for each agency accessing the N-DEx System. The NAC serves as the POC for the CSO at the local agency for matters relating to the N-DEx System. The NAC administers the N-DEx System for the local agency and oversees the agency's compliance with N-DEx System policies. The NAC may also be the agency's TAC. An agency may change its NAC at any time but must notify the CSA in writing of the change. The following N-DEx System roles may be performed by the CSO or delegated to the NAC or other appropriate personnel within the CSA or N-DEx System participating agency. It is recommended an alternate be assigned as a back-up to assist with performing the administrative duties in case of emergency or personnel changes. One individual may perform all administrative roles, or the roles may be assigned to several individuals.

1.6.4.1 **CSO Administrator Role** – Responsible for managing the users, audit, and training within their area of responsibility, as identified by ORI. The role is activated by the N-DEx Program Office within the N-DEx System for the CSO. Once activated, the role provides the CSO with the user, audit, and training management functionality. The CSO has the ability to assign the user, audit, and training management functionality by ORI to users or NACs at federal, state, local, and tribal agencies.

1.6.4.2 **Source Data Administrator (SDA) Role** – Responsible for establishing and managing the agency's configurable data sharing controls and submitting data to the N-DEx System for assigned record-owning agency(ies). The N-DEx Program Office enables the SDA capability within the N-DEx System.

1.6.4.3 **Automated Processing Administrator (APA) Role** – Responsible for activating, configuring, and managing the N-DEx System optional automated processing capability. Automated processing enables an agency to receive reports reflecting correlations between their submissions and current N-DEx System information.

1.7 System Security

1.7.1 The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, consistent with roles and responsibilities described in the *Bylaws for the CJIS Advisory Policy Board and Working Groups* and the *CJIS Security Policy*.

1.7.2 The FBI uses hardware and software controls to help ensure system security. However, final responsibility for the maintenance of the security and confidentiality of criminal justice information rests with the individual agencies participating in the N-DEx System. Further information regarding system security can be obtained from the *CJIS Security Policy*.

1.7.3 The data stored in the N-DEx System is documented criminal justice information and must be protected to ensure authorized, legal, and efficient dissemination and use. It is incumbent upon an N-DEx System participating agency to implement procedures to make the N-DEx System secure from any unauthorized use.

2.0 QUALITY CONTROL, VALIDATION, TRAINING, AND OTHER PROCEDURES

2.1 Maintaining System Integrity

2.1.1 Responsibility to Maintain System Integrity

2.1.1.1 Pursuant to the current version of the *Bylaws Of The Criminal Justice Information Services Advisory Policy Board And Working Groups,* the CSA is responsible for ensuring appropriate use, enforcing system discipline and security, and ensuring CJIS operating procedures are followed by all users, regardless of whether they are performed by CSA personnel, contracted support, an outside agency, etc.

2.1.1.2 A CSA may delegate responsibilities, including user management, to the NAC of subordinate agencies as outlined in the *CJIS Security Policy*.

2.1.1.3 The CSA may require notification of all new users given N-DEx System access through delegated user management. It is the CSA's responsibility to coordinate this notification process and the frequency of notification with the delegated "user management designee." This process will ensure the CSA has the desired level of involvement for user access since they remain ultimately responsible for all CJIS System of Services activities.

2.2 Security

2.2.1 Security standards are documented in the *CJIS Security Policy*.

2.3 Audit

2.3.1 Compliance audit: Compliance audit standards are documented in the *CJIS Security Policy*.

2.3.2 The FBI CJIS Division shall conduct compliance audits of CSAs which have agencies using the N-DEx System. Audits shall consist of the following:

2.3.2.1 Administrative interview with N-DEx System local agency NAC.

2.3.2.2 Network inspection.

2.3.2.3 A review of random N-DEx System transactions.

2.3.2.4 A review of user access.

2.3.2.5 Technical security and, if applicable, NCIC and III policies will also be assessed.

2.3.3 Audits will not include a review of data quality.

2.3.4 Security audits: Security audit standards are documented in the *CJIS Security Policy*.

2.3.5 Audits by the CSA: CSA audit responsibilities are documented in the *CJIS Security Policy* and Director approved APB guidance.

2.4 Training

2.4.1 CSAs may delegate N-DEx System training to local agencies or regional information sharing entities.

2.4.2 Prior to searching data via the N-DEx System, CSAs shall ensure, directly or through local delegation, users are trained on N-DEx System policy matters, emphasizing data use rules.

2.4.3 Basic security awareness training shall be required within six months of initial assignment and biennially thereafter, for all personnel who have access to criminal justice information.

2.4.4 Training shall be provided to N-DEx System users granted access to federated CJIS System of Services system(s) in accordance with individual federated system training requirements.

2.4.5 Every two years, users shall be trained on N-DEx System policy matters, emphasizing data use rules.

2.4.6 The CSA shall ensure all individuals with physical and logical access to N-DEx System information are trained on N-DEx System data use.

2.4.7 The CSA shall maintain records of all training and proficiency affirmation.

2.4.8 The N-DEx Program Office shall make training materials available to the CSA. Training materials may take the form of any of the below:

2.4.8.1 Basic course hand out materials and curriculum.

2.4.8.2 Video training.

2.4.8.3 Computer based training modules.

2.4.8.4 Distance Learning Workshops

2.5 Maintaining the Integrity of N-DEx System Records

2.5.1 Record-owning agencies are responsible for the timeliness, accuracy, and completeness of their data. The records in the record-owning agency record/case management system are considered the source records.

2.5.2 Timeliness: Each record-owning agency shall submit data, including any updates or changes to the original submission, as often as a contributor can feasibly execute them. Updates or changes shall be executed at least monthly.

2.5.3 Accuracy: Because records contributed to the N-DEx System will be limited to duplicates and summaries of records obtained and separately managed by the record-owning agency within its own record/case system(s), and for which the record-owning agency is responsible, each record-owning agency shall ensure contributed data is reflected within the source system(s). The record-owning agency shall ensure contributed data is synchronized with the agency's source system records as they are updated and changed.

2.5.4 Completeness: Each record-owning agency should submit as many N-DEx System data elements available and permitted by law.

2.6 Quality Control

2.6.1 FBI personnel periodically review records entered into the N-DEx System. Issues discovered in records are communicated directly to the CSA and NAC.

2.7 N-DEx System Maintenance

2.7.1 When scheduled maintenance is being conducted on the N-DEx System, an information page will be displayed stating the expected outage time. If the N-DEx System should become unavailable outside of scheduled maintenance times, a message notification banner will be displayed to the users. However, if the problem is not resolved after a reasonable period of time, notify the FBI CJIS Help Desk at 304-625-4357.

3.0 N-DEx SYSTEM SANCTIONS

3.1.1 In accordance with the *CJIS Security Policy*, each participating agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

3.1.2 Upon any discovery of misuse by any users or agencies granted access to the N-DEx System, notification to their NAC and CSA must take place immediately.

3.1.3 The CJIS APB established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits which are within the purview of the CES and detailed CES sanctions process procedures are available at <CJIS.gov> (Law Enforcement Enterprise Portal) CJIS Special Interest Groups /Advisory Process Information/Subcommittee/ CES Section and the CJIS Section of <FBI.gov>.

APPENDIX A: ACRONYMS

APA -	Automated Processing Administrator
APB -	Advisory Process Board
ATF -	Alcohol, Tobacco and Firearms
BRAG -	Bioterrorism Risk Assessment Group
CAU -	CJIS Audit Unit
CES -	Compliance Evaluation Subcommittee
CFR -	Code of Federal Regulations
CJA -	Criminal Justice Agency
CJIS -	Criminal Justice Information Services
CSA -	CJIS Systems Agency
CSO -	CJIS Systems Officer
CUI -	Controlled Unclassified Information
FBI -	Federal Bureau of Investigation
FFL -	Federal Firearm Licensee
IEPD -	Information Exchange Package Documentation
III -	Information Identification Index
LEA -	Law Enforcement Agency
LES -	Law Enforcement Sensitive
NAC -	N-DEx Agency Coordinator
NCIC -	National Crime Information Center
N-DEx -	National Data Exchange
NICS -	National Instant Criminal Background Check System
ORI -	Originating Agency Identifier
PII -	Personally Identifiable Information
PL -	Public Law
POC -	Point-of-Contact
SBU -	Sensitive But Unclassified
SDA -	Source Data Administrator
TAC -	Terminal Agency Coordinator
U.S. -	United States
U.S.C -	United States Code