



REQUEST FOR PROPOSAL

Title: NDI Expansion Project

Issue Date: **December 8, 2023**

Primary Contact: Victor McCraw

International Association of Directors of Law
Enforcement Standards and Training

152 S. Kestrel Pl.
Ste. 102
Eagle, ID 83616
Phone: (208) 288-5491
victor@iadlest.org

Responses Due: **February 5, 2024**



1 INTRODUCTION

The International Association of Directors of Law Enforcement Standards and Training is planning to expand the National Decertification Index as outlined in this Request for Proposal (RFP). The purpose of the National Decertification Index (NDI) is to serve as a national registry of certificate or license revocation actions relating to law enforcement officer misconduct. The International Association of Directors of Law Enforcement Standards and Training (IADLEST) intends to create and implement a best-in-class pointer system interactive database to empower NDI stakeholders to contribute and query information for the purpose of making informed hiring and employment decisions regarding previously employed law enforcement personnel and applicants.

IADLEST invites any information technology and management service providers that possess the ability and expertise to fulfill the requirements of this RFP to submit a response in accordance with the submission requirements and deadlines detailed in this RFP.

1.1 BACKGROUND

IADLEST is an international organization of training managers and executives dedicated to the improvement of public safety personnel. Every state in the United States has a state agency charged with setting the requirements which must be met to qualify (certify) a person as a law enforcement officer. These agencies are called POST (Peace Officer Standards and Training), or similar equivalent names related to their governing boards, commissions, or councils.

Created and administered by IADLEST, the NDI has been in continuous service in various iterations for 23 years. IADLEST developed the NDI 1999 and launched it as an online resource in 2000. Due to privacy concerns, the NDI 2.0 was launched in 2005 with a revised data structure to eliminate the use of Social Security numbers as identifiers. General references to the existing NDI in this RFP are references to NDI 2.0. References to the NDI in the future tense or specifically the NDI 3.0 refer to the NDI product which is the subject of this RFP.

The NDI contains basic information on officers against whom certification action has been initiated or taken. NDI data consists only of identifying information on the individual officer, the type of action taken, the reason for that action, and contact information for the reporting POST. POSTs hold complete detailed records with specifics about the exact nature, circumstances, and severity of officer misconduct. An NDI query which results in a match will “point” the user to the POST, where the officer’s full records are maintained. More information on the NDI program can be found by accessing the IADLEST website homepage at <https://www.iadlest.org/> and selecting the National Decertification Index logo.

1.2 NDI EXPANSION PROJECT MANAGEMENT

The Project Sponsor for the NDI Expansion Project is the U.S. DOJ, Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA). BJA guides the project at a strategic level, and has approved the scope, schedule, and budget. BJA’s guidance is based on Section Five of the May 2022 Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety.

The Executive Director of IADLEST serves as the Project Director and facilitates the project at a strategic and tactical level. Recommendations regarding the vendor selection or awards resulting from this RFP process will be escalated to the Project Sponsor for approval by the Project Director. The Project Director exercises oversight of the current NDI and is responsible for identifying the most effective NDI expansion solution, overseeing the expansion process, and establishing ongoing management of the NDI moving forward.

The Project Director has formed an NDI Expansion Advisory Committee (AC). The AC is comprised of POST executives, POST NDI users, law enforcement executives and representatives, and representatives from national law enforcement professional organizations. The AC is tasked with the development, distribution, and administration of this RFP, the evaluation of RFP responses, and the presentation of vendor recommendations to the Project Director.

1.3 TYPICAL NDI USAGE

Currently, the NDI points to cases involving the decertification, or loss of enforcement authority, of a law enforcement officer due to misconduct. There are a variety of situations which may result in the loss of a law enforcement officer's certification or lawful authority. Some circumstances are technical or purely administrative, such as failing to complete the yearly requirements for on-going training. The NDI is not intended to include these types of loss of certification, as they do not relate to misconduct. The NDI is intended to contain data on cases where officers are found to have moral flaws, commit acts of dishonesty, commit crimes or serious misconduct.

In such cases, the certifying authority (POST agency or Federal, State, Local, Tribal or Territorial agency [FSLTT]) will act according to its established protocols regarding discipline, certification status, and officer due process. If the certifying authority determines that a certification action is warranted (suspension, revocation, court-ordered relinquishment, etc.), or the officer decides to avoid such action by voluntarily relinquishing their certification, that agency will create a record in the NDI's computerized database.

The NDI may be queried by authorized law enforcement background investigators, law enforcement agency human resources personnel, and private organizations that provide employment background investigation services for pre-employment screening of new law enforcement recruits or lateral hiring of officers from other jurisdictions. Checking for NDI matches helps prevent the uninformed re-employment of law enforcement officers with a history of misconduct in other jurisdictions or states.

Basic informational reports are currently available as administrative functions of the NDI database. A Frequently Asked Questions (FAQ) file, and an NDI Brochure with a case study which illustrates the type of outcomes the database is designed to facilitate, is available by accessing the IADLEST website homepage at <https://www.iadlest.org/> and selecting the National Decertification Index logo.

CONTENTS

Appendi.....	1
1 INTRODUCTION.....	2
1.1 BACKGROUND.....	2
1.2 NDI EXPANSION PROJECT MANAGEMENT.....	2
1.3 TYPICAL NDI USAGE.....	3
2 PURPOSE.....	7
2.1 PROJECT OBJECTIVES.....	7
2.2 STAKEHOLDERS.....	8
3 PROJECT SCOPE AND DELIVERABLES.....	9
3.1 GENERAL OVERVIEW OF THE DESIRED SYSTEM.....	9
3.2 TECHNICAL OBJECTIVES.....	10
3.2.1 Technology Stack and Licenses.....	10
3.2.2 Security and Privacy.....	10
3.2.3 Privacy Impact Considerations.....	11
3.2.4 Data Architecture.....	12
3.2.5 Configurability and Changes.....	12
3.2.6 Dynamic Indexing.....	13
3.2.7 NDI Data Flow.....	13
3.3 SERVICE LEVEL AGREEMENTS (SLAs).....	15
3.3.1 General Usage.....	15
3.3.2 Specific SLAs.....	16
3.4 FUNCTIONAL DESIGN.....	16
3.4.1 User Management.....	17
3.5 NDI SYSTEM REQUIREMENTS.....	19
3.5.1 Main (Public) Dashboard.....	19
3.5.2 mail Alerts.....	19
3.5.3 IADLEST and POST Dashboards.....	20
3.5.4 Reporting.....	21
3.5.5 Future Expandability and Configurability.....	22
3.6 DATA MIGRATION.....	23
3.6.1 Existing NDI Data.....	23
3.6.2 New POST Agencies/Certifying Authorities.....	25

3.7	DEVELOPMENT.....	26
3.8	QUALITY ASSURANCE AND AUDITING	29
3.9	NDI DATA AND SYSTEM OWNERSHIP	29
3.10	INTERACTIVE USER ASSISTANCE AND DOCUMENTATION	29
4	TIMELINE AND BID SUBMISSION	30
4.1	PROCUREMENT AND EVALUATION PROCESS.....	30
4.1.1	Procurement Schedule and General Instructions.....	30
4.1.2	Proposal Submittal Address	31
4.1.3	Disposition of Material and Confidential or Proprietary Information	31
4.1.4	Proposal Preparation Costs.....	31
4.1.5	RFP Not a Contract.....	31
4.2	PRE-SUBMITTAL PROCESS.....	31
4.2.1	Request for Clarifications or Modifications	31
4.2.2	Ambiguity, Discrepancies, Omissions	32
4.2.3	RFP Addenda	32
4.3	SUBMISSION OF PROPOSALS	32
4.3.1	Proposal Delivery	32
4.3.2	Amendment or Withdrawal of Proposals	33
4.3.3	Mistake in Proposal.....	34
4.3.4	Error in Submitted Proposals	34
4.3.5	Validity Period of Proposals	34
4.3.6	Knowledge of Requirements.....	34
4.3.7	Independence of Proposal and Joint Proposals.....	35
4.3.8	Covenant Against Gratuities	35
4.3.9	Non-Disclosure and Conflict of Interest Acknowledgements	35
5	SELECTION CRITERIA	36
5.1	OVERVIEW OF EVALUATION PROCESS.....	36
5.1.1	Evaluation of Proposals.....	36
5.1.2	Reservation of Rights	36
5.1.3	Evaluation of Cost Proposal Sheets.....	37
5.1.4	Requests for Additional Information	37
5.2	QUALIFICATIONS.....	37
5.2.1	Minimum Qualifications.....	37

5.3	EVALUATION CRITERIA.....	38
5.4	INTERVIEWS, PRODUCT DEMONSTRATIONS, AND NEGOTIATIONS	38
5.4.1	Interviews.....	38
5.4.2	Interviews / Presentations / Demonstrations.....	39
5.4.3	Negotiations.....	39
5.5	PAYMENT	39
5.6	AWARD OF CONTRACT.....	39
5.6.1	Notification of Intent to Award Contract.....	39
5.6.2	Execution of Non-Disclosure Agreement.....	39
5.6.3	Execution of Contract.....	40
5.6.4	News Releases.....	40
Appendix 1:	NDI 3.0 SYSTEM FUNCTIONALITY AND ENHANCEMENTS	41
Appendix 2:	ANTICIPATED NDI 3.0 USER ACCESS LEVELS	44
Appendix 3:	SAMPLE ANTICIPATED WORKFLOW (Based on NDI 2.0).....	46
Appendix 4:	NDI 3.0 LOGGING REQUIREMENTS CHECKLIST	52

2 PURPOSE

The purpose of this project is to modernize and expand the functionality of the National Decertification Index (NDI). This expansion will include the design and implementation of state-of-the-art technology meeting the needs of IADLEST, state POST and similar organizations, and NDI users and stakeholders.

2.1 PROJECT OBJECTIVES

The NDI was created to promote professional accountability through transparency of information relating to misconduct by public safety personnel, to increase the public's trust in law enforcement, policing, and its public safety officers. To that end, the NDI 3.0 product will prioritize sustainability, affordability, data accuracy, and security to ensure that users have an experience that helps them build trust with the NDI and encourages adoption by law enforcement agencies.

Like the current NDI 2.0, the modernized NDI 3.0 with expanded functionality will also point to cases involving records of misconduct, criminal convictions, suspension of an officer's law enforcement authorities, terminations, and resignations or retirements while under investigation for serious misconduct or sustained complaints. Additionally, the NDI 3.0 will have the capability, when possible and permitted by law, to point to civil judgments against officers which are related to official duties (including amounts if publicly available), and records of disciplinary action based on findings of serious misconduct. As appropriate, the NDI may also hold information related to officer commendations and awards.

In service of this mission, the NDI Expansion Project will accomplish the following objectives:

- To further define the NDI as a nationally available resource that allows for the capture and sharing of accurate and timely information relating to actionable misconduct involving employed or certified public safety officers, or applicants for public safety positions (For the purpose of this objective, "actionable misconduct" is defined by the laws and rules that govern an individual's employment or certification as a public safety professional.)
- To encourage authorized law enforcement employers, recognized at the Federal, State, Local, Tribal or Territorial (FSLTT) levels, to utilize the NDI by reporting actions and/or searching NDI information prior to hiring individuals into a public safety position
- To provide users with data insights appropriate to their access-level through data dashboard visuals and exportable data
- To develop training and an NDI User Guide for user agencies

- To provide guidance to employers and certifiers of public safety personnel about when and how to make entry into the NDI to increase the consistency and reliability of the information contained within the NDI
- To increase the number of agencies contributing data to the system
- To increase the number of agencies using the system as part of their pre-employment investigation

2.2 STAKEHOLDERS

The NDI expansion must accommodate the needs of three general categories of NDI stakeholders:

Table 2-11: Stakeholders

STAKEHOLDERS		NEEDS
Upstream Stakeholders (Administrators)	<ul style="list-style-type: none"> • IADLEST 	The ability to access, control, monitor and extract NDI data for administrative and reporting purposes
Direct Stakeholders (Contributors)	<ul style="list-style-type: none"> • State POSTs • Current and future certifying authorities of individuals with police powers recognized nationally, locally, or territorially. • Other limited contributors 	The ability to enter information into the NDI regarding officer misconduct related to law enforcement matters and certification status
Downstream Stakeholders (Users)	<ul style="list-style-type: none"> • All direct stakeholders • Approximately 18,000 Federal, state, local, tribal, and territorial law enforcement agencies 	The ability to query NDI data and receive sufficient information to follow up on instances of confirmed or reported (under investigation) officer misconduct related to law enforcement matters and certification status
Public Stakeholders	<ul style="list-style-type: none"> • General Public • Researchers 	The ability to receive and review anonymized statistical reports compiled according to customizable parameters

3 PROJECT SCOPE AND DELIVERABLES

3.1 GENERAL OVERVIEW OF THE DESIRED SYSTEM

IADLEST intends the “new” National Decertification Index (NDI) to be a completely redesigned and reengineered secure web-based application. The NDI 3.0 will inherit the role of the current NDI and all of its functions, adding greater capacity and functionality. The web presentation will combine elements of a modernized database pointer system with user-configurable dashboards, graphical and analytical representations of data, and robust administrative and public reporting capabilities.

As a result of federal, state, and local initiatives to address the incidence of the retention and hiring of law enforcement personnel found to have previously violated standards of conduct, IADLEST anticipates a significant increase in reporting to the NDI. Additionally, several federal, national, state, local and tribal law enforcement agencies not governed by POST organizations are expected to begin reporting to the NDI. The NDI 3.0 will be capable of managing the increased volume of records and diversity of reporting authorities.

The NDI 3.0 will also establish procedures to ensure that the records stored in it are accurate, including by providing officers with sufficient notice and access to their records, as well as a full and fair opportunity to request amendment or removal of any information about themselves from the NDI on the grounds that it is inaccurate or that it is predicated on an official proceeding that lacked appropriate due process protections.

Note that this RFP uses the terms “POST,” “POST agency,” and “certifying authority” together and interchangeably to include non-POST federal law enforcement, military, or other Federal, State, Local, Tribal and Territorial (FSLTT) agencies identified by IADLEST as having authority over the law enforcement powers of individuals. There are an estimated 18,000 state, county, and municipal police agencies in the US, and numerous federal agencies employing individuals with law enforcement authority. The expanded NDI must have the capacity to accommodate users from all FSLTT law enforcement agencies.

The current National Decertification Index (NDI) has been in operation for several years. The web presentation currently consists of a database, dynamic web pages which interact with the database, and static web pages which are simply informational.

NDI records are entered by authorized POST agencies, and the system currently houses over **53,000** records. At the time of this RFP, about **11,000** users from various U.S. law enforcement agencies access the NDI.

3.2 TECHNICAL OBJECTIVES

3.2.1 TECHNOLOGY STACK AND LICENSES

The NDI 3.0 will be built on a modern tech stack that balances the security and maintenance benefits of existing tools with the long-term affordability of low licensing costs. The NDI 3.0 will be cloud-hosted with a preference for open-source software.

The NDI 3.0 tech stack shall not include proprietary systems that prevent IADLEST from working with another vendor to maintain the service in the future.

3.2.2 SECURITY AND PRIVACY

The security requirements of the NDI 3.0 include the following:

- The NDI must be tamper-proof and operate in accordance with modern data security standards, including industry standards and current federal data security requirements.
- The NDI platform must meet the FedRAMP and NIST 800-171 Moderate impact level requirements, although NDI will not be required to go through the FedRAMP authorization process as it is not a federal system.
- The NDI system must enforce the following access controls:
 - that Privileged users of the system's web application and system's computer devices (e.g., servers, network devices, databases, cloud management interfaces) must use phishing resistant multi-factor authentication (i.e., FIDO/WebAuthn authentication or public key infrastructure (PKI)-based).
 - Implement a minimum level of authentication for the non-privileged users of the system to require a temporary one-time code (TOTP) to a registered device, email, or phone number configured during initial account provisioning.
 - Support multiple MFA authentication options to include FIDO/WebAuthn for non-privileged users of the system who choose to use stronger authentication methods.
- The NDI activity log must record all data transactions to IADLEST standards (See Appendix 4). The activity log(s), including security-related events, shall be accessible and exportable for review by IADLEST on demand.

- Real-time data transaction monitoring and auditing with automated email notifications of suspicious activity is required. These notifications, which must include reporting within 1 (one) hour of incident discovery to info@iadlest.org, will be part of the NDI system automated email protocols.
- The NDI system will require a robust data backup system including off-site or secure cloud storage of database contents, as well as an up-to-date version of the web pages such that restoration of a ransomware encrypted hard drive or other malware breach can be quickly resolved and a clean system brought back online with minimum downtime.
- The NDI system will apply security patches for Critical and High vulnerabilities within 30 days, Moderate with 90 days.
- The NDI system will use a dependency auditing framework or tool (e.g., OWASP) for automated security review of versioned dependencies.
- The NDI system will be required to initiate credentialed vulnerability enumeration scans every 14 days.
- The NDI must update vulnerability detection signatures on the scanning tool within 24 hours from the last vendor-released signature update.
- The NDI must establish an ISA with all parties accessing the NDI system that will include the type of connection, roles and responsible data protection requirements, incident management, vulnerability management, and contingency plan.
- The NDI system must implement encryption for data in transit and data-at-rest.
- The NDI system shall incorporate privacy-by-design best practices including collecting only the information necessary to fulfill the purpose of the system, restricting access to information to those with a need to know, and appropriately disposing of data once it is no longer needed.

3.2.3 PRIVACY IMPACT CONSIDERATIONS

The NDI will be required to conduct a privacy impact assessment prior to deployment of the system which identifies and sufficiently mitigates any privacy risks.

To protect the privacy of the individuals identified in the NDI, the NDI will require sufficient identifying information of the querying party prior to displaying a responsive record.

3.2.4 DATA ARCHITECTURE

The desired data structure of the NDI 3.0 database will be a Master Name Index, based on each subject for whom data exists, or is entered, in the NDI.

The system should link each subject to all associated action record(s) entered for the subject.

- Each individual who is a subject of NDI record(s) must be uniquely identified in the system.
- The unique NDI subject identifier will serve as a tool for indexing data and verifying matches with search criteria.
- The identifier assigned to each subject must be non-sensitive data. Social Security numbers are NOT an option.
- To the extent possible, the system should link records across states and data sources.

3.2.5 CONFIGURABILITY AND CHANGES

Upon the authorization of IADLEST, there will occasionally need to be changes to the database configurations such as adding, removing, or editing data fields; changing user access permissions, and adding new search parameters. To the extent practicable, IADLEST's NDI administrators should have the ability to make basic changes themselves without contractor involvement.

The contractor shall include basic configuration changes or provide optional pricing for complex changes in the maintenance period of the system. Changes made by the contractor shall occur within a reasonable timeframe appropriate to the request.

The NDI data fields will be editable, with the ability to add new user access levels, and add or discontinue data fields and data input selection options. This includes the ability to customize fields, metadata, indexing options, and data entry and search parameters, without compromising subject records created with previous combinations of notifications, actions, and reasons.

There is also a need to create conditionally required fields. For example, if an action is entered for which the reason is "Civil Judgement," a required field should appear prompting the entry of a dollar amount, or a comment with details about the judgement if the amount is unavailable. For this reason, the NDI 3.0 will need a database field change log to systematically record all modifications to data fields, including updates, deletions, and additions, along with the identity of the administrator making the change, and the timestamp.

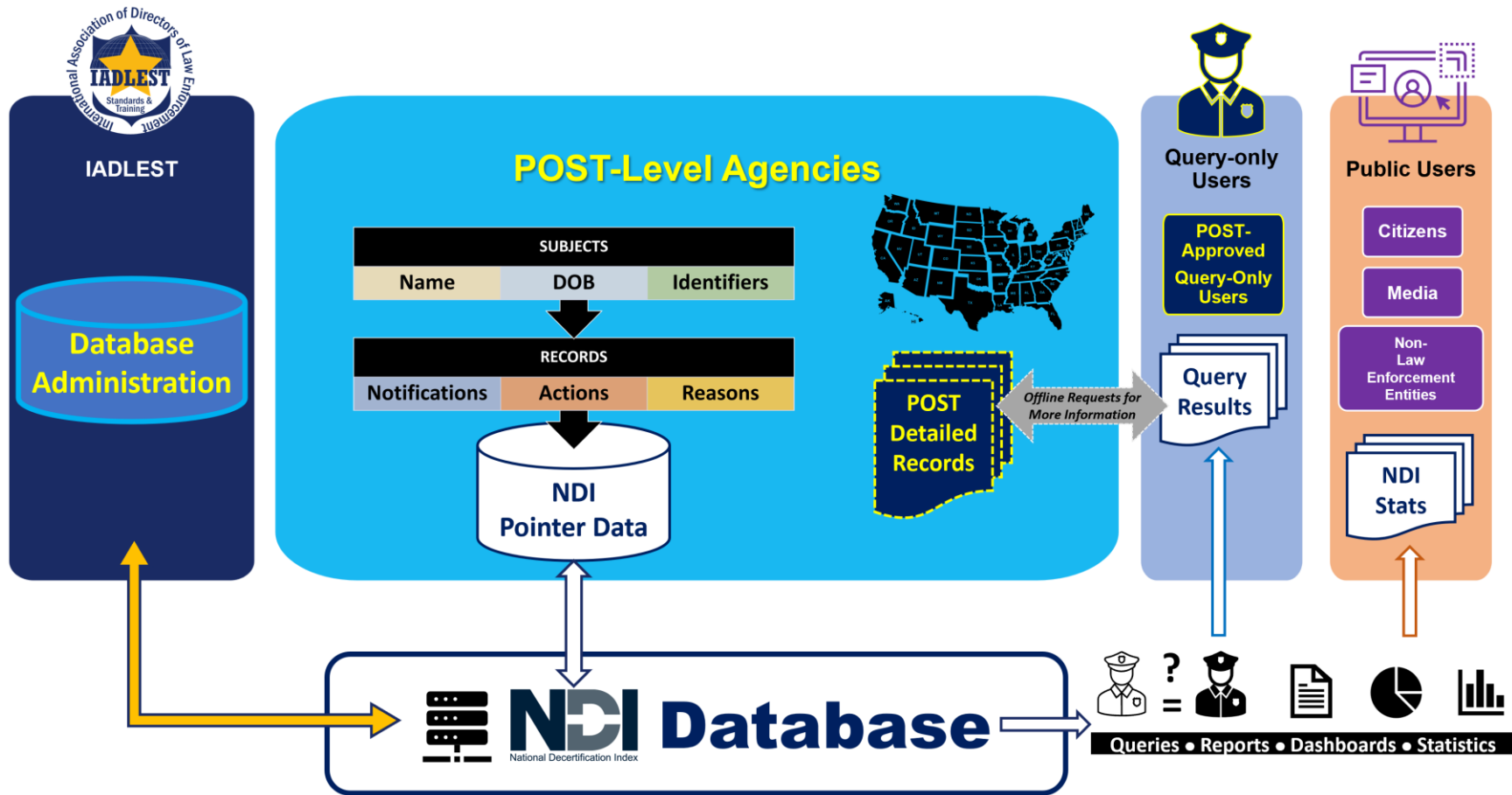
3.2.6 DYNAMIC INDEXING

The NDI 3.0 database should have the ability to dynamically create and update indexes as new data is added or modified. This could include automatic indexing of new data or the ability to manually trigger indexing.

3.2.7 NDI DATA FLOW

The data management and data entry and query functions of the NDI should follow the general flow of data illustrated in Figure 3-1.

Figure 3-1: NDI General Data Flow



3.3 SERVICE LEVEL AGREEMENTS (SLAs)

3.3.1 GENERAL USAGE

Bandwidth requirements for the existing system are modest, although we anticipate a 10x upsurge in usage as more local police departments and federal agencies begin using the NDI. Figure 3-2 is a screenshot showing usage of the NDI system for a two-week period in October 2023. The figure includes website access and usage statistics like NDI record searches (bottom row), webpage section views, POST administrative activity, and other usage metrics.

The NDI 3.0 system must be reliable, thoroughly tested, scalable, and capable of handling the anticipated increase in usage and traffic. Not only will the volume and frequency of NDI usage increase, the content and types of data are likely to change or expand to comply with future national law enforcement reform requirements. Statistics like those shown in Figure 3-2 must be accurate and readily reportable at any time with flexible and configurable data visualization options.

Figure 3-2: NDI System Usage Data

135	IADLEST > Our Services > NDI	26
136	IADLEST > Our Services > NDI > About NDI	2,851
137	IADLEST > Our Services > NDI > Admin > Action Types	7
138	IADLEST > Our Services > NDI > Admin > Actions	72
139	IADLEST > Our Services > NDI > Admin > Actions > Edit	44
140	IADLEST > Our Services > NDI > Admin > Applications	238
141	IADLEST > Our Services > NDI > Admin > Member List - Admin	39
142	IADLEST > Our Services > NDI > Admin > Member List - Admin > Edit	24
143	IADLEST > Our Services > NDI > Admin > Organizations	62
144	IADLEST > Our Services > NDI > Admin > Organizations > Edit	35
145	IADLEST > Our Services > NDI > Admin > POST Users	123
146	IADLEST > Our Services > NDI > Admin > POST Users > Edit	19
147	IADLEST > Our Services > NDI > Admin > Reasons	8
148	IADLEST > Our Services > NDI > Admin > Subjects	87
149	IADLEST > Our Services > NDI > Admin > Subjects > Edit	25
150	IADLEST > Our Services > NDI > POST Dashboard	55
151	IADLEST > Our Services > NDI > Report Action	162
152	IADLEST > Our Services > NDI > Request NDI Access	851
153	IADLEST > Our Services > NDI > Search NDI	3,368

3.3.2 SPECIFIC SLAS

The NDI 3.0 shall meet the following SLAs:

- The system shall be available 99.9% of the total minutes in each calendar month in the production environment, and 99% in all other environments (excluding scheduled outages)
- Scheduled service outages shall not exceed 2 consecutive hours in the production environment
- The contractor shall notify IADLEST within 15 minutes of any unplanned service outage
- Services shall begin recovery within 15 minutes of any unplanned service outage
- Services shall be available at 100% of capacity within 6 hours of any unplanned service outage
- Security incidents with potential impacts to availability, confidentiality, or integrity shall be reported no more than 1 hour following detection
- Critical vulnerabilities and emergency patches shall be deployed within 24 hours for vulnerabilities known to be exploitable that do not have mitigating controls in place
- Non-emergency security vulnerability patching shall be ever 30 calendar days
- Security vulnerabilities that have mitigating controls in place shall be corrected within 30/60/90 days depending on severity of High/Medium/Low
- The contractor shall resolve bugs within the following time frames from bug discovery:
 - High Level: 3 business days
 - High impacts such as unreachable service, unavailability of primary functions, or privacy and security breaches
 - Medium Level: 5 business days
 - Medium impacts such as unavailability of secondary functionality or medium degradation of service
 - Low Level: 30 business days
 - Low impacts such as slight degradation of response time, functionality is available with workarounds, or cosmetic issues
- The contractor shall retain weekly backups for a minimum of 1 month
- The contractor shall restore the system from backup within 1 business day from a request from IADLEST.
- Email alerts shall be sent within 1 minute of generation

3.4 FUNCTIONAL DESIGN

As a simple, but robust, database pointer system, the NDI 3.0 will facilitate the creation/registration of users with specified levels of access and system permissions, the entry of records tied to uniquely identified subjects with standardized information fields, and the query or retrieval of subject data for individual matches and statistical reporting.

The design of the NDI 3.0 will be consistent with modern and innovative data management and control, based on human-centered design best practices. The pages of the NDI 3.0 will be formatted for responsive viewing on common internet-capable devices.

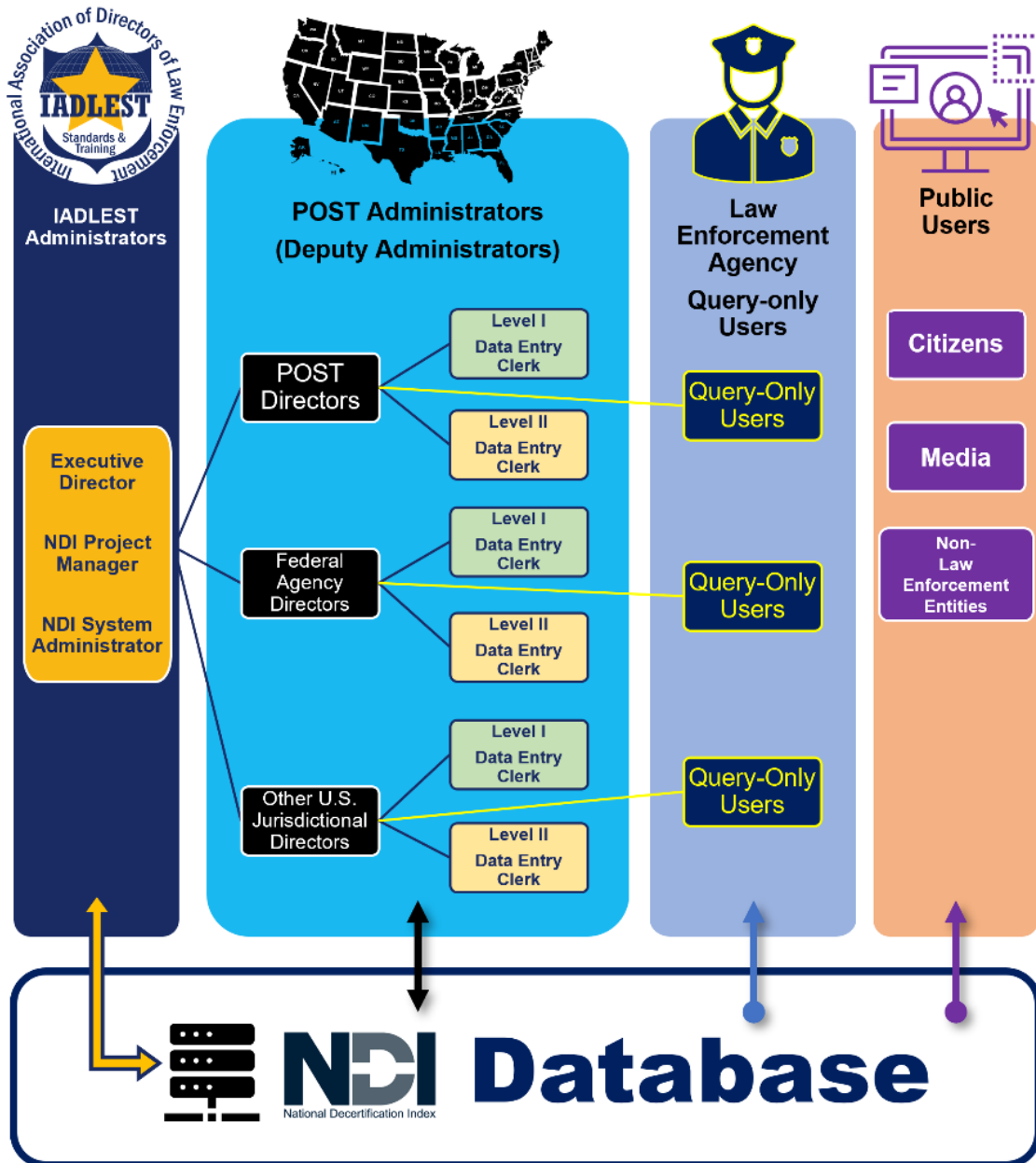
3.4.1 USER MANAGEMENT

IADLEST NDI Administrators will oversee the NDI, and delegate user access level approvals to the appropriate POST agency or authority.

POST Agency Administrators 'own' all of the records for their state or jurisdiction. They may create Data Entry Users and Query-only Users.

In addition to support for multiple operational access and permission levels, the NDI will accommodate an option for public access to anonymized data. The functions related to the management of NDI user levels of access and permissions and the entry of data conform to the system illustrated in Figure 3-3.

Figure 3-3: NDI User Management Hierarchy



The anticipated user access levels and permissions are described in Appendix 2 of this RFP.

3.5 NDI SYSTEM REQUIREMENTS

3.5.1 MAIN (PUBLIC) DASHBOARD

The NDI home/login/landing page will serve as a promotional tool for the system, and a resource for individuals coming to the system seeking information about peace officer certifications, training requirements, and qualifications for access to the NDI system. The overall aesthetic of the main page will be modern and facilitate innovative data management and control, with a user experience-centered design. IADLEST Administrators will have the ability to edit this page to reflect changes in certifications and requirements going forward.

The public-facing dashboard must be visually appealing, user-friendly, easy to navigate, and conform with industry standards for accessibility. The dashboard will include user-configurable graphical and analytical representations of data, and access to public reporting capabilities.

The main page will include a secure, yet user-friendly, login process which recognizes the user's level of access and presents a secondary system dashboard which allows authorized transactions only.

Dashboards shall integrate dynamic visualization of NDI data appropriate for user access level and user needs.

3.5.2 MAIL ALERTS

The NDI 3.0 system will include the ability to generate email alerts for certain transactions such as timely notifications, reminders, and system status updates. This capability should be sufficiently configurable to accommodate future user communication needs.

Examples of emails to be included are:

- NDI New User Application Received
 - Sent to the applicant
 - Sent to IADLEST Administrator
- NDI New User Application Notification to Supervisor
 - Sent to Applicant's Supervisor
- NDI – New User Application Needs Review
 - Sent to POST or Certifying Authority contact for the applicant's state
 - Sent to the email list established by an IADLEST Administrator as described in Appendix 3, "Request Access."

- NDI New User Application Approved
 - Sent to Applicant
 - Sent to IADLEST Administrator
- NDI New User Application Denied
 - Sent to Applicant
 - Sent to IADLEST Administrator
- POST Agencies will receive periodic reminders of New User applications waiting in queue for review and approval/denial
- NDI Reminder - Pending New User Applications Need Approval (time sensitive)
 - Sent to POST contact for each state with applications in queue without approval or denial for a specified length of time
 - Sent to IADLEST Administrator
- NDI Reminder – Notifications, Suspensions, Probations (time sensitive)
 - Sent to POST contact for each state for records which have not been updated after a specified length of time after being entered as Notifications of subjects under investigation
 - Sent to POST contact for each state for records which have not been updated after a specified length of time after being entered as Suspensions or Probations of subjects' peace officer authority
 - Sent to IADLEST Administrator
- NDI POST User Summary
 - Sent to each POST detailing activity of each authorized user in that state
- NDI Organization Added
 - Sent to IADLEST Administrator when New User Applicant adds a new organization

3.5.3 IADLEST AND POST DASHBOARDS

The IADLEST and POST Administrator dashboards will include a robust data interface which displays statistical NDI data metrics. Various levels of record detail will be available, down to the details of individual subject records, with the ability to export data to common file formats. The dashboards shall be designed based on user research and usability testing to meet user needs.

- ***IADLEST Administrators' Dashboard***

The IADLEST Administrators' dashboard will display data and reporting options for EVERY state and jurisdiction, including all data transactions and records, and system

usage metrics. The IADLEST Administrators' dashboard will facilitate the appropriate user tasks and workflows for an administrator, including but not limited to:

- maintenance of all levels of user access and permissions, including POST Administrators (described below)
- management of email functionality
- data exportation and analysis

- ***POST Administrators' Dashboards***

The POST Administrators' dashboards will display data and reporting options for ONLY their state or jurisdiction, including their state/jurisdiction's data transactions and records, and system usage metrics. The POST Administrators' dashboards will facilitate the appropriate user tasks and workflows for their access level, including but not limited to maintenance of levels of user access and permissions for their state/jurisdiction's Level I and II Data Entry Clerks, and Query-Only Users.

3.5.4 REPORTING

The NDI 3.0 will support the ability to filter results on any NDI data attributes and generate configurable data visualizations for dashboards, reports, and statistical data outputs. Automated reports should be suitable to meet the administrative needs of IADLEST and state POST organizations.

NDI 3.0 query-level users will have the immediate ability to download, save and/or print a formatted PDF NDI Query Report of a check on an individual. The report will contain the identity of the NDI user and the date and time of the record check and will include either the NDI data retrieved for the individual, or a confirmation that no NDI record(s) exist for the individual.

IADLEST and POST NDI Administrators will be able to create and save custom reports and visualizations that are relevant to their specific analytic needs.

The NDI 3.0 system will include functionality for aggregated data, query, and output using an authenticated query service. This service will be used to support data requests from investigative service providers, internal data review, and the external analysis of census, demographic, crime statistics, and other data from national databases.

Automatic and on-demand IADLEST Administrator and POST auditing of the activities of each user under their jurisdiction to support the monitoring of system usage, and to prevent and deter unauthorized use.

3.5.5 FUTURE EXPANDABILITY AND CONFIGURABILITY

Nothing in the design and programming should preclude the potential future expansion and configuration of the NDI.

3.6 DATA MIGRATION

3.6.1 EXISTING NDI DATA

The NDI 3.0 system must accommodate the migration of over 53,000 records and approximately 10,500 user profiles from 11,200 different U.S. law enforcement agencies in the current system with 100% fidelity, while preserving, updating, or archiving previous data fields to match the new data configuration.

NDI 3.0 records will conform to the following updates in available Action types:

Table 3-1: NDI "Action" Types

ACTIONS	
CURRENT NDI ACTIONS	NDI 3.0 ACTIONS
Old Type	New Type
Denied	Certification/Licensure Denied
Judgment	None. This action will not be available for future records. [Records with this action will be retained and available by search]
Suspended for Cause	Suspended This is a time-bound Action which will trigger an email alert to review records with this Action after a specified period of time, and to update the Action type if appropriate. [Clarify with the information button that this is a certification suspension, not a suspension from duty]
None. [New term]	Probation This is a time-bound Action which will trigger an email alert to review records with this Action after a specified period of time, and to update the Action type if appropriate. [Clarify with the information button that this is a certification probation, not a new probationary employee status]
Reinstatement	Reinstatement
Relinquishment	Relinquishment [Note: "Voluntary Relinquishment" also exists as a Reason to further confirm the voluntary surrender of certification]
Revoked for Cause	Revoked
Under Review/Investigation	None. This Action will not be available for future records. Existing records will be designated as a "Notification" (Table 3-3).
NOTE: Future configurable categories of actions, and action types within those categories will be a requirement of the NDI 3.0 system.	

NDI 3.0 records will conform to the following updates in available Reason types:

Table 3-2: NDI "Reason" Types

REASONS	
CURRENT NDI REASONS	NDI 3.0 REASONS
Old Type	New Type
Executive Review	POST Administrative Review
Felony Conviction	Felony Conviction
Judicial Appeal	Judicial Order
Legislative/Statutory	None. This reason will not be available for future records. [Records with this Reason will be retained and available by search]
Misconduct	Misconduct
Misdemeanor Conviction	Misdemeanor Conviction
Other	None. This reason will not be available for future records. [Records with this Reason will be merged with Other/Unspecified and be available by search under that reason]
Other/Unspecified	Other/Unspecified
Terms Met	None. This reason will not be available for future records. [Records with this Reason will be retained and available by search]
Voluntary Relinquishment	Voluntary Relinquishment
<i>None.</i> [New term]	Criminal Judgment
<i>None.</i> [New term]	Civil Judgment*
* Will trigger a required field to appear prompting the entry of a dollar amount, or a comment with details about the judgement if the amount is unavailable.	
NOTE: Future configurable categories of actions, and action types within those categories will be a requirement of the NDI 3.0 system.	

No existing NDI records have an associated Notification field(s). NDI 3.0 records will include a field option or options for “Notification.” Notification types will include the following, and the system should accommodate additional notification types in the future:

Table 3-3: NDI 3.0 "Notification" Categories

NOTIFICATION(S)	
Type	Considerations
Under Review/Investigation	<ul style="list-style-type: none"> • This Notification will exist in the form of a “Yes or No” checkbox. • This Notification may be selected for any NDI record, with or without an Action or Reason. • An entry in the Comment field will be required for this Notification. • This Notification designation will trigger a periodic Email Alert as a reminder to POST associated with the NDI record to reevaluate and update the record. • This is a time-bound Notification which will trigger an email alert to review records with this Notification after a specified period of time, and to update the record type if appropriate. <p>[Clarify for persons who enter or query records that this Notification is only an indication that due process proceedings have been initiated]</p>
<p><i>NOTE: Future configurable categories of actions, and action types within those categories will be a requirement of the NDI 3.0 system.</i></p>	

3.6.2 NEW POST AGENCIES/CERTIFYING AUTHORITIES

NDI 3.0 contributor agencies, and law enforcement certifying authorities that are not yet contributing to the NDI, may have historical records. The system must provide an adaptable mechanism for automated batch data migration into the NDI with error mitigation.

3.7 DEVELOPMENT

The RFP Selectee will include a database pointer system development plan, outlined in their RFP response. IADLEST expects that the plan will include at least the equivalents of the following phases, each with timelines within the overall project plan.

Table 3-4: Project Phases

PROJECT PHASE	DEVELOPMENT PHASE	GENERAL DESCRIPTION
Discovery Phase	Requirement analysis and prioritization	<p>IADLEST will provide the RFP Selectee with full technical information and usage statistics regarding the current NDI system.</p> <p>The RFP Selectee will conduct an analysis to identify the specific system characteristics required to fulfill the functionality and volume of data needs of the NDI.</p> <p>The RFP selectee will work with IADLEST to prioritize functionality of the new system and define a Minimum Viable Product (MVP) and data migration strategy to launch the new system into production and a roadmap to full functionality.</p>
	Database design	The RFP Selectee will present one or more database models capable of meeting the requirements of the NDI.
	Evaluation and selection	The RFP Selectee will evaluate the potential database management systems choices in coordination with IADLEST and choose the one which best suits the requirements of the NDI.
	Ongoing Discovery	<p>Throughout the development phase, the RFP selectee will include ongoing discovery to understand user need.</p> <p>Throughout the development, the RFP selectee will conduct usability tests with users to ensure that the system meets their needs and inform future development requirements</p>

PROJECT PHASE	DEVELOPMENT PHASE	GENERAL DESCRIPTION
Design Phase	Logical database design	Once the evaluation and selection development phases are completed, the RFP Selectee will develop an internal model which includes mapping of all objects, i.e., design of tables, indexes, views, transactions, access privileges, information security, etc.
Development Phase	MVP Implementation	The RFP Selectee will coordinate with IADLEST to implement the NDI 3.0 system.
	MVP Data loading	<p>Once the database has been created, the existing NDI data must be migrated into the database with 100% fidelity (no loss of data or accessibility).</p> <p>The RFP Selectee will perform the required data conversion if the existing data is in a different format than required for the NDI 3.0.</p>
	MVP Testing and performance tuning	<p>The RFP Selectee will coordinate with IADLEST to thoroughly test the operation and functionality of the NDI 3.0.</p> <p>This phase includes the collection of new data, modifying existing data, and archiving of obsolete data.</p> <p>This phase includes the debugging period in which programming bugs will be fixed, minor tweaks made to the presentation, and additional reports or pages requested.</p>
	Operation	The RFP Selectee will coordinate with IADLEST to “go-live” with the NDI 3.0. In this phase, the system will be accessed by the end users and application programs.
	Iterative Development	Once the MVP is live, the RFP selectee will continue delivering functionality on the NDI 3.0 until all functionality in the contract is delivered.

PROJECT PHASE	DEVELOPMENT PHASE	GENERAL DESCRIPTION
<p align="center">Product Management Phase</p>	<p align="center">Maintenance</p>	<p>This is an ongoing phase of the NDI 3.0 system.</p> <p>The major tasks included are:</p> <ul style="list-style-type: none"> • Database backup and recovery • Access management • Hardware maintenance • Application of security patches • Bug-fixing • Upgrades to database and programming software

3.8 QUALITY ASSURANCE AND AUDITING

The NDI 3.0 will have both automated and on-demand functions dedicated to the monitoring of information flow, system efficiency, system usage, record counts, trends, and auditing for information integrity and identification of misuse or security issues. Configurable QA and audit report functions will be available for IADLEST Administrators.

3.9 NDI DATA AND SYSTEM OWNERSHIP

All data in the NDI 3.0 system is the sole property of IADLEST and shall not be used for any purposes other than those listed in the NDI contract.

The NDI system code and configurations are the property of IADLEST. The NDI 3.0 system will be constructed such that IADLEST retains a fully functional and operable system should the vendor relationship be terminated, or the vendor be unable to continue maintenance. Should the IADLEST-vendor relationship end, the vendor will support the transition of maintenance services to a new vendor.

3.10 INTERACTIVE USER ASSISTANCE AND DOCUMENTATION

The NDI 3.0 must include an integrated, context-sensitive virtual user guide designed to provide on-screen information prompts and interactive on-demand help functions. This system shall be intuitive, enabling users to receive guidance and instructions relevant to the specific module, screen, or function they are utilizing. The guide should anticipate common user queries and provide step-by-step assistance for database operations, ranging from basic navigation to query formulation. The on-demand help should be accessible via easily identifiable icons or a dedicated help menu within the application's user interface, and capable of providing real-time, relevant assistance without significant disruption to the user's workflow.

Additionally, the NDI 3.0 will include a downloadable, detailed PDF comprehensive user manual that encompasses all aspects of the database software's functionality. This document should be structured logically, with a clear table of contents, index, and searchable keywords to allow users to quickly locate information. High-quality screenshots, diagrams, and flowcharts must be included to illustrate processes, with stepwise instructions for each user feature and operation. The comprehensive manual should be written in clear, concise language that is accessible to users with varying levels of technical expertise. It must be thorough enough to serve as both a training resource for new users and a reference tool for experienced users. The PDF should be regularly updated to reflect database updates or changes.

4 TIMELINE AND BID SUBMISSION

4.1 PROCUREMENT AND EVALUATION PROCESS

4.1.1 PROCUREMENT SCHEDULE AND GENERAL INSTRUCTIONS

- A. IADLEST has developed the following list of key events from RFP issuance through notice of contract award. All key dates are subject to change at IADLEST’s discretion.

Table 4-1: RFP Timeline

EVENT	Key Dates
RFP Publication	12/8/2023
Virtual RFP Overview and Question/Answer Session	1/8/2024
Deadline for Vendor Requests for Clarifications or Modifications	1/16/2024
IADLEST Posts Clarification / Modification Response	1/22/2024
Proposal Due Date and Time (Midnight Pacific Time)	2/5/2024
Preliminary Evaluation of Proposals (estimated)	2/5/2024 – 2/26/2024
Notification of Vendors Selected to Make Oral Presentations / Interviews (estimated)	2/29/2024
Oral Presentations (estimated)	3/18/2024 – 3/22/2024
Final Evaluation (estimated)	3/25/2024
Negotiations (estimated)	3/25/2024 – 3/31/2024
Notice of Intent to Award (estimated)	4/1/2024
Execution of Contract (estimated)	April 2024

- B. This RFP and any addenda that may be issued will be available on the following website:

<https://www.iadlest.org/our-services/ndi/about-ndi>

(“IADLEST website NDI page”)

4.1.2 PROPOSAL SUBMITTAL ADDRESS

Email: info@iadlest.org

Subject: **NDI RFP Response**

4.1.3 DISPOSITION OF MATERIAL AND CONFIDENTIAL OR PROPRIETARY INFORMATION

All materials submitted in response to this RFP will become the property of IADLEST and will be returned or deleted only at IADLEST's option and at the expense of the vendor submitting the proposal. [A record of a submitted proposal will be retained for official files and may become public record. Any material that a vendor considers as confidential and not specifically required by the RFP should not be included in the vendor's proposal as it may be made available to the public.]

4.1.4 PROPOSAL PREPARATION COSTS

Vendors submitting proposals do so entirely at their expense. There is no express or implied obligation by IADLEST to reimburse a vendor for any costs incurred in preparing or submitting proposals, providing additional information when requested by IADLEST, participating in any selection interviews or product demonstrations, or participating in this procurement.

4.1.5 RFP NOT A CONTRACT

The RFP does not constitute a contract or an offer of employment. IADLEST reserves the right to make one award, multiple awards, or to reject all proposals, in whole or in part, submitted in response to this RFP. IADLEST further reserves the right to make no award, and to modify or cancel, in whole or in part, this RFP.

4.2 PRE-SUBMITTAL PROCESS

4.2.1 REQUEST FOR CLARIFICATIONS OR MODIFICATIONS

- A.** Vendors interested in responding to this RFP may submit questions by e-mail only on procedural matters related to the RFP or requests for clarification or modification of this RFP document, to the designated Proposal Submittal Address (Section 4.1.2). If the vendor is requesting a change, the request must set forth the recommended change and the vendor's reasons for proposing the change.
- B.** All questions and requests must be submitted by email to the designated Proposal Submittal Address email box no later than the date specified in in this RFP (Section 4.1.1.A). Questions or requests submitted after the due date will not be answered.
- C.** All email submissions sent to the designated Proposal Submittal Address **MUST** contain the email subject line: **NDI RFP Response**. Failure to indicate that the submission is an NDI RFP Response in the email subject line may result in IADLEST taking no action on a vendor's email submission.

- D. Without disclosing the source of the question or request, IADLEST's NDI Project Manager will post a copy of the questions and IADLEST's responses on the IADLEST website NDI page.

4.2.2 AMBIGUITY, DISCREPANCIES, OMISSIONS

- A. If a vendor submitting a proposal discovers any ambiguity, conflict, discrepancy, omission, or other error in this RFP document, the vendor shall immediately provide written notice of the problem by email to the designated Proposal Submittal Address and request that the RFP document be clarified or modified. Without disclosing the source of the request, IADLEST may modify the RFP document prior to the date fixed for submission of proposals by posting the addendum on the IADLEST website NDI page.
- B. If prior to the date fixed for submission of proposals a vendor submitting a proposal knows of or should have known of an error in the RFP document but fails to notify IADLEST of the error, the vendor shall propose at its own risk, and if the vendor is awarded the contract, the vendor shall not be entitled to additional compensation or time by reason of the error or its later correction.
- C. Written notification of any ambiguity, conflict, discrepancy, omission, or other error in this RFP document submitted after the Proposal Due Date will not be responded to by IADLEST.

4.2.3 RFP ADDENDA

- A. IADLEST may modify the RFP document prior to the date fixed for submission of proposals by posting an addendum on the IADLEST website NDI page. If any potential vendor determines that the addendum unnecessarily restricts its ability to propose, it must notify IADLEST via email at the designated Proposal Submittal Address no later than three (3) business days following the date the addendum is posted on the IADLEST website NDI page.
- B. Each vendor's proposal, including prices/costs offered, shall reflect the requirements of IADLEST including all addenda issued by IADLEST. Failure to do so will permit IADLEST to interpret the proposal to include all addenda issued in any resulting contract.

4.3 SUBMISSION OF PROPOSALS

4.3.1 PROPOSAL DELIVERY

- A. Proposals must be delivered via email to the designated Proposal Submittal Address listed in Section 4.1.2 no later than the Proposal Due Date and Time specified in Section 4.1.1.A.
- B. Proposal must be submitted in **two parts** as follows:

1. Provide a project **technical proposal**, signed by an authorized representative of the vendor, and including the name, title, address, and telephone number of one individual who is the vendor's designated representative. The technical proposal **must not include any pricing information.**

There are no restrictions on the length of the technical proposal, however the proposal of products or services outside of the scope of this RFP will not be considered during the evaluation.

The project technical proposal should include a **proposal summary** of no more than three pages. Although there are no restrictions on the length of the technical proposal itself, the summary must not be more than three pages.

2. Provide a project cost/fee proposal, signed by an authorized representative of the vendor. The cost/fee proposal must be submitted in a separate electronic document titled "**Cost Proposal**," and must include the name, title, address, and telephone number of one individual who is the vendor's designated representative.

The Cost proposal needs to clearly separate design/development costs from ongoing maintenance costs.

- C. All proposals must be received via email on or before the Proposal Due Date and Time. Proposals received prior to the Proposal Due Date and Time that are marked properly will be securely kept and will remain unevaluated until the Preliminary Evaluation of Proposals.
- D. **PROPOSALS RECEIVED AFTER THE PROPOSAL DUE DATE AND TIME WILL NOT BE CONSIDERED.**
- E. The Vendor is solely responsible for ensuring that the full proposal is received by IADLEST in accordance with the RFP requirements, prior to the Proposal Due Date and Time, and at the email specified. IADLEST shall not be responsible for any email system restrictions or outages, or for delivery errors or delays or missed delivery.
- F. Submittal of proposals by facsimile or physical mail delivery is not acceptable, and any proposal so transmitted will be rejected as non-responsive.
- G. Submittal of proposals to any email address other than the Proposal Submittal Address may result in the rejection of proposal as being non-responsive.

4.3.2 AMENDMENT OR WITHDRAWAL OF PROPOSALS

- A. A vendor may amend its proposal prior to the Proposal Due Date and Time. All amendments must be received by IADLEST prior to the Proposal Due Date and Time. Amended proposals must comply with all proposal submission requirements set forth herein. In addition, the amendment email subject line must be clearly state

“Amended Proposal.” In the event a vendor submits an amended proposal prior to the Proposal Due Date and Time, the vendor’s original proposal will not be considered for evaluation. **AMENDED PROPOSALS RECEIVED AFTER THE PROPOSAL DUE DATE AND TIME WILL NOT BE CONSIDERED.**

- B. A vendor may withdraw its proposal at any time prior to the Proposal Due Date and Time by notifying the Proposal Submittal Address of its withdrawal. The withdrawal must be signed by a duly authorized officer of the vendor.
- C. Amendments or withdrawals offered in any other manner, oral or written, will not be considered. Proposals cannot be amended or withdrawn after the Proposal Due Date and Time.

4.3.3 MISTAKE IN PROPOSAL

If after Proposal Due Date and Time but prior to a contract award, a Vendor discovers a mistake in their proposal that renders the Vendor unwilling to perform under any resulting contract, the Vendor must immediately notify IADLEST and request to withdraw the proposal. The notice shall be addressed to the Proposal Submittal Address, signed by a duly authorized officer of the Vendor, and sent to the designated Proposal Submittal Address email. It shall be solely within IADLEST’s discretion as to whether withdrawal will be permitted.

4.3.4 ERROR IN SUBMITTED PROPOSALS

- A. If an error is discovered in a vendor’s proposal, IADLEST may at its sole option retain the proposal and allow the Vendor to submit certain corrections. IADLEST may, at its sole option, allow the Vendor to correct obvious clerical errors. In determining if a correction will be allowed, IADLEST will consider the conformance of the proposal to the format and content required by the RFP, the significance and magnitude of the correction, and any unusual complexity of the format and content required by the RFP.
- B. If the Vendor’s intent is clearly established based on review of the complete proposal submitted, IADLEST may, at its sole option, allow the Vendor to correct an error based on that established intent.

4.3.5 VALIDITY PERIOD OF PROPOSALS

Proposals will be valid for ninety (90) days after the Proposal Due Date specified in Section 4.1.1.A. In the event a final contract has not been awarded by the date specified in Section 4.1.1.A, IADLEST reserves the right to negotiate extensions to the Proposal Validity Date.

4.3.6 KNOWLEDGE OF REQUIREMENTS

- A. The vendor shall carefully review the RFP documents, and all documents referenced and made a part of the RFP document to ensure that all information required to properly respond has been submitted or made available and all requirements are

priced in the proposal. Failure to examine any document, drawing, specification, or instruction will be at the Vendor's sole risk.

- B. Vendors shall be responsible for knowledge of all items and conditions contained in their proposals and in this RFP, including any IADLEST-issued clarifications, modifications, amendments, or addenda. IADLEST will post addenda and clarifications to the NDI webpage; however, it is the Vendor's responsibility to ascertain that its proposal includes all addenda issued prior to the Proposal Due Date.

4.3.7 INDEPENDENCE OF PROPOSAL AND JOINT PROPOSALS

- A. Unless a Vendor is submitting a joint proposal, the Vendor represents and warrants that by submitting its proposal it did not conspire with any other vendor to set prices with the intent to influence this RFP process.
- B. A proposal submitted by two or more vendors participating jointly in one proposal may be submitted, but one vendor must be identified as the prime contractor and the other(s) as the subcontractor. IADLEST assumes no responsibility or obligation for the division of payments, authorized expenses if allowed by the subsequent contract, or responsibilities among joint contractors.

4.3.8 COVENANT AGAINST GRATUITIES

Vendor warrants by signing its proposal that no gratuities, in the form of entertainment, gifts, or otherwise, were offered by the Vendor or any agent, director, or representative of the Vendor, to any officer, official, agent, or employee of IADLEST, the U.S. DOJ, or NDI Advisory Committee member(s) with a view toward securing award of or securing favorable treatment with respect to any determinations concerning the performance of any resulting contract. For breach or violation of this warranty, IADLEST will have the right to terminate any resulting contract in whole or in part. The rights and remedies of IADLEST provided in this provision shall not be exclusive and are in addition to any other rights and remedies provided by law or under the resulting contract.

4.3.9 NON-DISCLOSURE AND CONFLICT OF INTEREST ACKNOWLEDGEMENTS

Vendors responding to this Request for Proposal may be required at any time during the process to submit non-disclosure and/or conflict of interest attestations or documentation deemed necessary by the Project Sponsor for the NDI Expansion Project: the U.S. DOJ, Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA).

5 SELECTION CRITERIA

5.1 OVERVIEW OF EVALUATION PROCESS

5.1.1 EVALUATION OF PROPOSALS

- A. IADLEST will conduct a comprehensive, fair, and impartial evaluation of proposals received in response to this RFP. All proposals received from vendors will be reviewed and evaluated by a committee of qualified personnel (the “NDI Advisory Committee”). The name, units, or experience of the individual members will not be made available to any vendor or requestor at any time prior to, during, or after this RFP.
- B. Proposals meeting the Minimum Qualifications set forth in this RFP will be distributed to the NDI Advisory Committee.
- C. The NDI Advisory Committee will first review and complete the evaluation of the project technical proposals without the cost proposal. As set forth in Section 4.3.1.B, technical proposals must not contain any pricing information. Project technical proposals that contain pricing information may be rejected as being non-responsive and may not receive further consideration.
- D. Upon completion of the project technical proposal evaluations, cost proposals will be reviewed, and evaluated to determine an overall evaluation score.

5.1.2 RESERVATION OF RIGHTS

- A. IADLEST, in its complete discretion, may also eliminate proposals that have not met the minimum qualifications of the RFP, or have not scored adequately in relation to other proposals to warrant further consideration. IADLEST reserves the right to reject any or all proposals, in whole or in part, and may or may not waive any immaterial deviation or defect in a proposal. IADLEST’s waiver of an immaterial deviation or defect shall in no way modify the RFP document or excuse a vendor from full compliance with RFP document specifications.
- B. If a proposal fails to meet a material RFP document requirement, the proposal may be rejected. A deviation is material to the extent that a response is not in substantial accord with the requirements of the RFP document. Material deviations cannot be waived.
- C. IADLEST reserves the right to negotiate with Vendors who have presented the best proposal, in the opinion of the NDI Advisory Committee, in an attempt to reach an agreement. If no agreement is reached, IADLEST can negotiate with other Vendors or make no award under this RFP. At any time, the NDI Advisory Committee can reject all proposals and make no award under this RFP. Moreover, IADLEST reserves the right to reconsider any proposal submitted at any phase of the procurement. It also reserves the right to meet with vendors to gather additional information.

- D. Proposals that contain false or misleading statements may be rejected if in IADLEST's opinion the information was intended to mislead IADLEST regarding a requirement of the RFP document.

5.1.3 EVALUATION OF COST PROPOSAL SHEETS

Cost/fee proposals will be reviewed only if a proposal is determined to be otherwise qualified. All figures entered in the cost proposal must be clearly represented. Cost proposal sheet content should include at a minimum the cost of each Project Phase outlined in Section 3.7, Table 3-4, taking into account each associated Development Phase or equivalent vendor-specific process.

5.1.4 REQUESTS FOR ADDITIONAL INFORMATION

IADLEST reserves the right to seek clarification or additional information from any Vendor throughout the RFP process. IADLEST may require a Vendor's representative to answer questions during the evaluation process regarding the vendor's proposal. Failure of a Vendor to demonstrate that the claims made in its proposal are in fact true may be sufficient cause for deeming a proposal non-responsive.

5.2 QUALIFICATIONS

5.2.1 MINIMUM QUALIFICATIONS

A. Vendors should meet the minimum qualification requirements listed below.

1. Vendor has completed at least two (2) projects of comparable size and scope anticipated by this RFP.
2. Neither vendor nor any of its proposed subcontractors are currently under suspension or debarment by any state or federal government agency and neither vendor nor any of its proposed subcontractors are tax delinquent with the any state or the Federal Government.

B. The Vendor must state specifically in its Executive Summary how it meets or complies with each minimum qualification specified in the RFP. Subject to IADLEST's right, in its sole and complete discretion, to waive minor deviations or defects, only those proposals that meet all the foregoing minimum qualifications shall be considered for a full evaluation and a possible contract award.

5.3 EVALUATION CRITERIA

Proposals will be evaluated to determine the proposal that offers the best value to IADLEST and the Project Sponsor. The evaluation will be based upon the following criteria, listed in order of descending priority (although some factors are weighted more than others, all are considered necessary, and a proposal must be technically acceptable in each area to be eligible for award):

- A. Ability of proposed technology stack to meet IADLEST requirements
- B. Ability of vendor to configure and/or customize the NDI for IADLEST requirements
- C. Scope and quality of proposed technical and maintenance support offered during the Development Phase, implementation through operation.
- D. Quality and appropriateness of the proposed execution of the Product Management Phase maintenance and support contract
- E. Overall reasonableness of fee proposal (Not based strictly on lowest bid)
- F. Ability to meet timing requirements to complete the project (One (1) year from the date of the contract award for the purpose of this RFP.) This project completion time may later be adjusted at the discretion of IADLEST with notice to the selected vendor
- G. References

5.4 INTERVIEWS, PRODUCT DEMONSTRATIONS, AND NEGOTIATIONS

5.4.1 INTERVIEWS

- A. Following the initial screening of proposals, IADLEST reserves the right to request, and each Vendor must be prepared to conduct oral presentations and other discussions (written or verbal) on the content of its proposal. If IADLEST determines that interviews or presentations are required, selected Vendors will be notified in writing of the date, place, time and format of the interview or presentation. Vendors will be responsible for all costs related to the interview, which, at IADLEST's sole discretion, may be in-person and/or by teleconference. If selected to participate in an interview or presentation, a Vendor's failure to participate in such interviews or presentations shall result in a Vendor's disqualification from further consideration.
- B. Interviews, if held, are designed to provide IADLEST with clarification of submitted proposals only, and shall not be construed as a solicitation, invitation, or opportunity for vendors to alter, modify, or amend their previously submitted proposals. Any alterations, modifications or amendments offered shall not be considered by IADLEST; but will, however, be viewed as negatively impacting the interview evaluation.

- C. Each vendor must ensure that a minimum of one of its project managers and one technical lead personnel attend the interview.

5.4.2 INTERVIEWS / PRESENTATIONS / DEMONSTRATIONS

Following the initial screening of proposals, IADLEST will identify the vendors selected to continue in the RFP process. IADLEST will notify the selected vendors in writing and work with each vendor to arrange a time and place for the interviews, presentations, and/or demonstrations. Each selected vendor should be prepared to participate in an interview, presentation, and/or demonstration as deemed necessary by IADLEST, per the schedule documented in Section 4.1.1.A. If requested to participate in an interview, presentation, and/or demonstration, a vendor's failure to do so may result in disqualification from further consideration.

5.4.3 NEGOTIATIONS

If IADLEST desires to enter into negotiations, they will do so with one or more Vendors, at IADLEST's sole discretion. If IADLEST enters into negotiations and no agreement is reached, IADLEST can negotiate with the other Vendors or make no award under this RFP. IADLEST reserves the right to award a contract, if any, without negotiations.

5.5 PAYMENT

Payment terms will be specified in any contract that may ensue as a result of this RFP document. IADLEST DOES NOT MAKE ANY ADVANCE PAYMENT FOR GOODS OR SERVICES. Payment for the services anticipated by this RFP will be on cost reimbursement basis, up to a specified not to exceed amount, inclusive of all authorized expenses, and will be made based upon completion of tasks, or the acceptance of deliverables, as provided in the agreement between IADLEST and any selected vendor.

5.6 AWARD OF CONTRACT

5.6.1 NOTIFICATION OF INTENT TO AWARD CONTRACT

The NDI Advisory Committee will make a final recommendation for the award of the contract to IADLEST. The Program Director will subsequently issue a Notice of Intent to Award to all Vendors by posting the Notice of Intent to Award on the IADLEST website NDI page. IADLEST reserves the right to award, in whole or in part, to make multiple awards, or to make no award and to modify or cancel, in whole or in part, this RFP.

5.6.2 EXECUTION OF NON-DISCLOSURE AGREEMENT

Upon award, the intended awardee may be required to submit non-disclosure attestations or documentation deemed necessary by the Project Sponsor for the NDI Expansion Project: the U.S. DOJ, Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA).

5.6.3 EXECUTION OF CONTRACT

Upon award, the intended awardee will be required to adhere to the terms and timeframes of the contract.

5.6.4 NEWS RELEASES

News releases pertaining to the award of any contract resulting from this RFP may not be made by a vendor without the prior written approval of IADLEST Executive Director in coordination with U.S. DOJ.

APPENDIX 1: NDI 3.0 SYSTEM FUNCTIONALITY AND ENHANCEMENTS

DESIRED NDI SYSTEM FUNCTIONALITY AND ENHANCEMENTS

Enhancements of the newly modified and expanded NDI will include the following features and capabilities. Throughout the discovery and development process, the contractor may propose alternatives that better meet the overall objectives of the project and the needs of the users:

NDI Record Entry

IADLEST Administrators must have the ability to designate levels or categories of NDI contributors (those agencies permitted to make record entries), and the capability to add, delete, merge, or edit NDI contributors' levels, categories, names, contributed content, and other information. For continuity and record integrity, a log of administrator actions must be maintained.

The automated aggregation of a drop-down list of authorized NDI contributor agencies, and a list of suggested existing agency names upon request to enter a new agency name, or similar features are strongly desired.

NDI contributors will be presented with a user experience that permits the assignment of Notifications, Actions, Reasons, and Comments regarding investigations and certification status changes for subjects they enter into the NDI.

In cases of serious alleged misconduct, where due process proceedings have commenced but may take many months, the NDI will support the creation of an "Under Review/Investigation" notification record. This record will be similar in configuration to all other NDI records, with the option to be updated by the reporting POST upon the finalization of the Action, and clearly displayed and reported separately from records where due process is complete. The automated notification emails described in Section 3.5.2 and Table 3-3 will include a periodic reminder to the reporting POST to update the "Under Review/Investigation" notification record status.

In cases of serious misconduct, where due process proceedings have been completed and the Action taken is suspension or probation (non-permanent certification action), the NDI will support the creation of a "Suspended" or "Probation" record. This record will be similar in configuration to all other NDI records, with the option to be updated by the reporting POST upon a change of certification status to Reinstatement, Revoked, etc. The automated notification emails described in Section 3.5.2 and Table 3-1 will include a periodic reminder to the reporting POST to update the "Suspended" or "Probation" record status.

IADLEST Administrators must be able to define and establish interrelated selections of Actions and Reasons.

The entry of duplicate or conflicting records should be disallowed, with considerations for the NDI contributors' ability to:

- delete, or request deletion, of a record,
- revise or update an existing record, and
- create subsequent record(s) for the same subject.

Each individual who is a subject of NDI record(s) must be uniquely identified in the system. The identifier assigned to each subject must be non-sensitive data. Social Security numbers are NOT an option. (See Section 3.2.4)

Maximize the capability for contributing agencies to automate data entry via manual entry APIs, batch CSV uploads, or similar method which checks for quality and completeness of submitted record data.

NDI Record Queries

The NDI will be accessible to record queries by authorized users.

Each new NDI query user will be authorized in the system by the appropriate unique POST organization, federal agency, or other certifying authority which oversees the certification, peace officer authority, or law enforcement function for their jurisdiction.

Each new NDI query user will be assigned in the system to a unique law enforcement agency within the jurisdiction of authorizing POST level organization.

The entry of duplicate or conflicting agency information for query users should be disallowed (e.g., Boise Police Department, versus Boise Police Dept., versus Boise PD, versus Boise City Police Dept., etc.). The system must feature an aggregated drop-down list of recognized agencies, and a list of suggested existing agency names upon request before a new agency name is created. This will aid in preventing duplicate agency entries.

NDI record queries will be the most frequently used feature of the NDI, and mechanisms to ensure fast, accurate and complete record search results are a requirement.

Both match and near match results should be returned for each query. The unique NDI subject identifier will serve as a tool for verifying matches with search criteria.

Match, near match, and no match results will be clearly indicated, with a user option to generate, save, and print an NDI Query Report with a digital date and time stamp.

Reporting

The NDI must include reporting functions with the ability to filter results on any NDI attributes. Report output options must include on-screen data visualization and configurable report formats for download.

NDI queries will generate an NDI Query Report configurable by IADLEST Administrators, which may be saved and/or printed by the user as verification of the date, time, and result details of the query.

The NDI system will allow users to create and save custom reports and visualizations that are relevant to their specific analytic needs.

Advanced data handling and reporting functions will provide for the analysis of multiple internal and external data sets based on linked keys. This may include census, demographic, crime statistics, and other data from federal databases.

The system will facilitate automatic and on-demand IADLEST Administrator and POST auditing of the activities of each user under their jurisdiction. This will serve as an indication of how the system is being used in each state and as a security measure to prevent and deter unauthorized use. The following types of information must be readily accessible:

The frequency and quantity of subject records entered into the NDI

How often the NDI is queried

How many subject query matches are detected

Automated anonymized reports should be configurable by IADLEST Administrators to meet the administrative needs of stakeholders.

APPENDIX 2: ANTICIPATED NDI 3.0 USER ACCESS LEVELS

ANTICIPATED NDI USER ACCESS LEVELS

These are the anticipated user access levels required in the NDI 3.0. Throughout the discovery and development process, the contractor may propose alternatives that better meet the overall objectives of the project and the needs of the users.

A. IADLEST Administrators:

1. May create new POST-level agencies
2. May create any level of system user
3. May add, delete, read all records in system
4. May add, delete, or edit Action Types and Reasons
5. May add, delete, or edit any NDI user/member
6. May add, delete, or edit any auto-generated emails
7. May add, delete, or edit any agencies in the system
8. May add, delete, or edit any POST-assigned to agencies or companies
9. May add, delete, or edit any POST Administrators (as described below)

B. POST Administrators:

1. May create Level 1 and Level 2 Data Entry Users for their state (defined below)
2. May add and delete records (only for their state or jurisdiction)
3. May read all records in system
4. May review and approve Query-only Users for their state

C. Level 1 POST Data Entry Clerk:

1. May add records for their state
2. May delete records for their state
3. May read all records in system

D. Level 2 POST Data Entry Clerk:

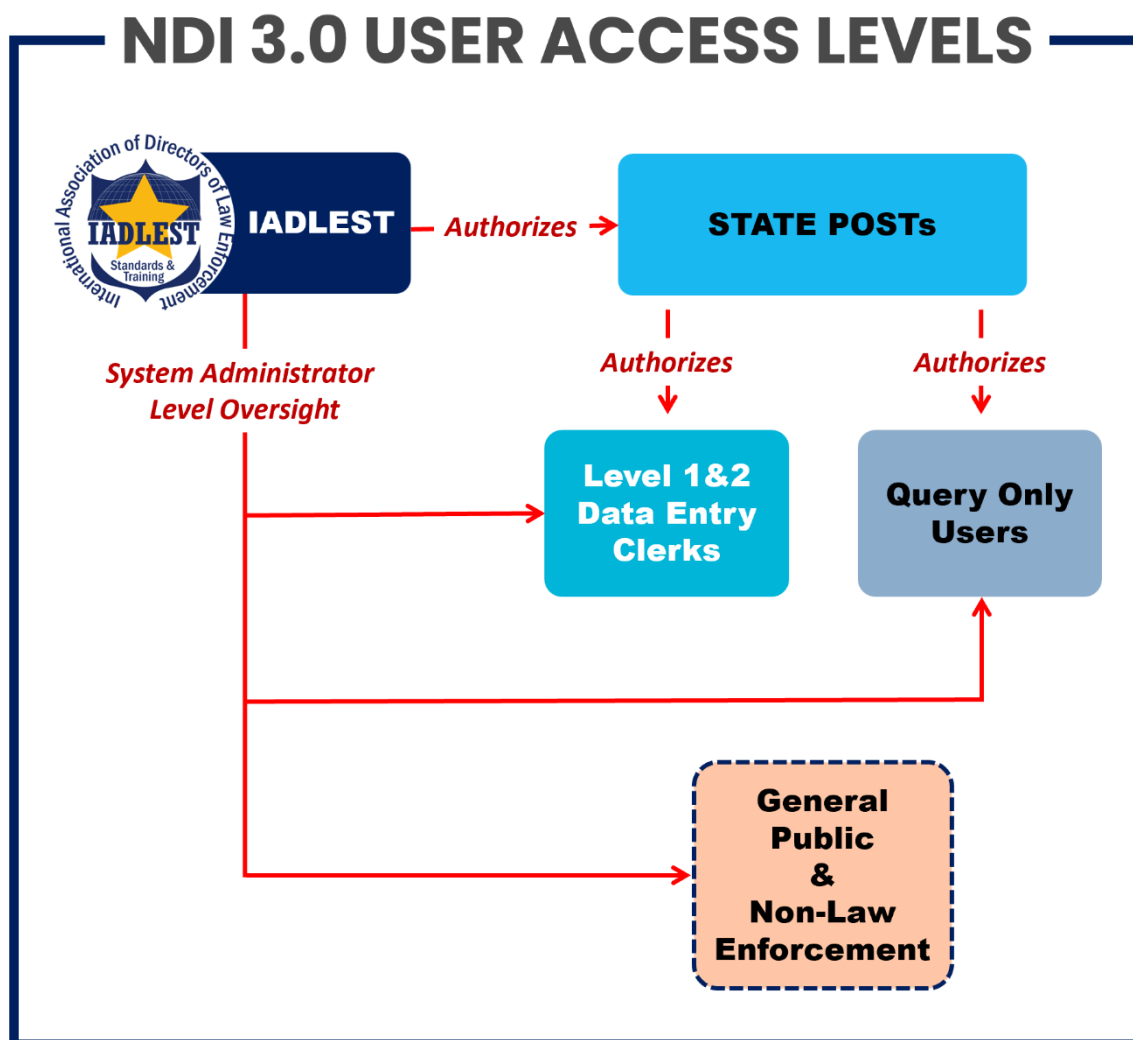
1. May add records for their state
2. May NOT delete records for their state
3. May read all records in system

E. Query-only User:

1. Authorized by each state POST
2. May read all records in system

- F. General Public and Non-Law Enforcement User:
1. May view the public facing dashboard
 2. May enter parameters to generate different visualizations of dashboard data
 3. May enter parameters to access anonymized data via preformatted reports

Figure A2-1: Basic Relationship Between User Access Levels



APPENDIX 3: SAMPLE ANTICIPATED WORKFLOW (BASED ON NDI 2.0)

SAMPLE ANTICIPATED WORKFLOW

These are the anticipated user workflows required in the NDI 3.0. Throughout the discovery and development process, the contractor may propose alternatives that better meet the overall objectives of the project and the needs of the users.

Login and Access Request

The main NDI page will serve as a login portal and will display a configurable public facing dashboard. Information on this page will explain the criteria for NDI system access (a legitimate law enforcement need, subject to verification and approval by the state POST agency or certifying authority).

Login

The NDI “Login” function will include prompts for approved and registered users’ email (username) and password, and an automated “Reset Password” option. To log in, a user’s profile and organization must have previously been entered into the system and approved by the state POST agency or certifying authority.

Request Access

A “Request Access” function will be available for new (unapproved) users. There needs to be a mechanism to avoid duplicate access requests by the same individual, and to detect requests for access from an individual who already has access privileges. Reapplications by previously denied applicants should trigger a notification and override option for IADLEST Administrators. The following information will be collected on the New User application form:

USER PROFILE	
Title	
First Name*	
Middle Initial	
Last Name *	
Email *	
Phone *	
License/Cert. #	
Organization	☰
Supervisor Name *	
Supervisor Email*	
Supervisor Phone	
Comment	

Fields marked with an asterisk (*) are required. The “Email” field will require the applicant to verify their correct email address by entering it twice.

The “Comment” field will be a text field with sufficient space to allow for a short paragraph.

The User Profile entry function will prevent duplicate user entries.

The “Organization” field will allow for a picklist selection, and an option to “Search for Organization.” The “Search for Organization” selection will reveal the following search term inputs:

- Name*
- Country
- State

The access applicant may enter a partial name in the required organization Name field, and the system will return all organization names in that state which match. The applicant may then select the name of their organization.

If the access applicant's organization does not already exist in the system, a "My Organization Is Not Listed" selection will be available, which will display a "New Organization" form with the following fields:

ORGANIZATION	
Name	
Country *	☰
Address (Line 1)	
Address (Line 2)	
City *	
State *	
Postal Code *	
Phone Number *	
Website URL	
Organization Type *	☰
Supervising POST *	☰

The "Organization Type" picklist displays the following options:

- Academy
- Agency
- Company

The "Supervising POST" picklist will be populated with state POST agencies and certifying authorities authorized in the applicant's state or jurisdiction. Certifying authorities will include non-POST federal law enforcement, military, or other agencies identified by IADLEST, and IADLEST will have the ability to create, delete, and merge records for certifying authority organizations without the loss of existing data.

Saving the completed "New Organization" form submits the organization record for IADLEST Administrator review and approval prior to establishing the record in the database. The act of saving the form will alert the IADLEST Administrator via email that a new organization request is awaiting review. This new organization approval process should detect and alert IADLEST Administrators of the potential unintentional duplication of existing organizations in the system. Duplicate records compromise the accurate submission and retrieval of NDI information. For example, an NDI access applicant of the St. Petersburg Police Department, might enter the organization name as: St. Pete PD, St. Petersburg PD, SPPD, etc. IADLEST Administrators should have the ability to create, delete, merge, and migrate organizations and the records associated with each organization, without the loss of existing data.

Each successful submission of a new NDI user request for access will trigger an automatic email to be sent to the email list established by an IADLEST Administrator as described in Section 3.5.2.

Data Entry Management

- **Entering Certification Actions or Events**

Basic Data Process Considerations

When a POST data entry clerk enters a record, the data entry will be minimal. Currently, when an individual is entered in the system, they are identified by Last Name, First Name, and Date of Birth. The use of Social Security numbers is NOT acceptable for identification in the NDI. (See Section 3.2.4)

An “Action” is selected from a pull-down list, then a corresponding “Reason” is selected from another pull-down list. There is an optional comment field where additional brief details may be entered. The POST agency retains the detailed documents regarding the case. As a result, each NDI data record will be very small.

A law enforcement officer may lose their certification for a variety of reasons. They may also be suspended pending completion of due process, or have their certification reinstated upon administrative or judicial review. Depending on the circumstances, a POST data entry clerk may choose to:

enter an Action and a Reason for the certification action, or
enter only a “Notification” indicating that the officer’s conduct is under review or investigation.

The process of reporting certification actions or events must accommodate these three options for each record entry. This process is described in detail below. All data entry selections available to Data Entry Clerks will be supported by an accessible “help” or “information” function with guidance and/or details about the selection.

- **Reporting Actions**

Subject Information

Data entry clerks will have the option to select a “Report Action” menu item, which will display an input window with a “Subject Information” form with the following input fields:

SUBJECT (Match?)
Last Name *
First Name
Date of Birth* [mm/dd/yyyy]

(Fields marked with an asterisk () are required.)*

The system will automatically search for subject matches and display the results. The purpose of this input step is to reduce the chance of unintentionally creating a duplicate subject record in the NDI. If the subject has not been previously entered in the NDI (no match), the system will

display a “Create a New Subject” button. Clicking the button will display an input window with a “Create Subject” form, prompting the Data Entry Clerk to enter the following fields:

Create New SUBJECT
First Name *
Middle Name
Last Name *
Maiden Name
Suffix
AKA [Also Known As]
Date of Birth * [mm/dd/yyyy]

- **Entering Notifications**

The NDI 3.0 system will include a list of “Notification” options which may be applied to a record entry in conjunction with an Action and Reason, or independently. The “Under Review/Investigation” notification is an initial need. Future configurable notification types will be a requirement of the system.

The following is an example of Notification options:

NOTIFICATION
Under Review/Investigation <input checked="" type="checkbox"/>
[Configurable]* Yes <input checked="" type="checkbox"/> No <input checked="" type="checkbox"/>
[Configurable] <input checked="" type="checkbox"/>
Comment *

The “Under Review/Investigation” notification applies to situations where Action is pending the completion of due process.

Future NDI records may be associated with other temporary or descriptive statuses or attributes. The ability to create notification types and the ability to identify, track, and report records with specific notifications is desirable. An informational pop-up should appear upon checking any Notification box requiring the data entry clerk to verify the appropriate conditions apply before opening the “Comment” field.

The “Comment” field entry is required for all “Notification” choices. The “Comment” field will be a text field with sufficient space to allow for a short paragraph.

- **Entering Actions**

Depending on the action taken regarding an officer’s certification, the data entry clerk may select the appropriate action type from the following list:

ACTION
Cert./License Denied
Judgment
Suspended
Reinstatement
Relinquishment
Revoked

Future configurable categories of actions, and action types within those categories will be a requirement of the system.

The “Reason” options will be presented to the data entry clerk upon selection of an “Action.”

- **Entering Reasons**

The NDI 3.0 system will include the following reason types for actions. The Reason selections will be conditional depending upon the Action selected. Example: The “POST Administration Review” selection will only be selectable if “Reinstatement” is selected as the Action.

The following are the “Reason” types:

REASON
POST Administration Review
Felony Conviction
Judicial Order
Misconduct
Misdemeanor Conviction
Voluntary Relinquishment
Criminal Judgment
Other/Unspecified

A “Reason” selection of “Other/Unspecified” will require an explanatory entry in the “Comment” field.

Future configurable reason types within action categories and action types will be a requirement of the system.

Database Queries

- **NDI Searches**

The most frequent NDI data transaction is the query. This transaction must be simple, fast, and reliable. NDI Users seeking to query the database are presented with a search comprised of a “Last Name” field, with the option of including advanced search parameters, including “First Name” and a range for Date of Birth.


NDI Search Results

Searches on a Last Name will return a list of names including the key word input in the search field. For example, a search on the Last Name “Smith” will yield individuals with the last name matching “Smith” as well as “Goldsmith,” “Smithson,” etc.

The database will initially return the contents of the “Last Name,” “First Name,” “Date of Birth,” and a count of the number of Actions associated with that individual.

The NDI User may click on the entry in the returned results to see more detail for each record associated with the identified subject.

This will result in the following fields being displayed:

NDI Pointer Data	
SUBJECT INFORMATION	
NOTIFICATION(S)	
ACTION	
REASON	
POST Agency	

Subject Information

- First Name
- Middle Name
- Last Name
- Maiden Name
- Suffix
- AKA
- Date of Birth
- Notification
- Action
- Reason [with View button]
- POST Agency

The NDI User may click on the 'View' button, which will display additional information, including:

- Service Dates
- Certification Information
- POST Contact Name
- POST Contact Phone
- Comments

APPENDIX 4: NDI 3.0 LOGGING REQUIREMENTS CHECKLIST

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
1	Host logging	<p>If Endpoint Detection and Response (EDR) is installed on a host (i.e., devices running Windows, Linux/*nix, or MacOS operating system), telemetry events and audit records generated by the EDR platform must be captured.</p> <p>Or if there is no EDR on a host, log all security events, system events, authentication events, program execution events, scripting events made available via operating system configuration.</p>	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
2	Recursive Domain Name System (DNS)	<p>Collect logs which capture the details of all DNS queries and responses originating from within the system boundary/environment. Examples of the minimum data/level of detail that must be included (this is not an exhaustive list):</p> <ul style="list-style-type: none"> - Source of request (IP address, hostname, etc.) - Source of response (IP address, hostname, etc.) - ID of recursive server logging the data (IP address, hostname, etc.) - Query Size in Bytes - Response Size in Bytes - Time to Live (TTL) value associated with response - Protocol (UDP, TCP or Both) for request - Protocol (UDP, TCP or Both) response 	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
3	Authoritative DNS	<p>Collect logs which capture the details of all DNS queries and responses sent to authoritative/resolving DNS servers within the system boundary/environment. Examples of the minimum data/level of detail that must be included (this is not an exhaustive list):</p> <ul style="list-style-type: none"> - Source of request (IP address, hostname, etc.) - Source of response (IP address, hostname, etc.) - ID of recursive server logging the data (IP address, hostname, etc.) - Query Size in Bytes - Response Size in Bytes - Time to Live (TTL) value associated with response - Protocol (UDP, TCP or Both) for request - Protocol (UDP, TCP or Both) response <p>In addition, zone transfer requests and responses must be logged to include the data capturing the details of the request and the response as well as the contents of any such requests.</p>	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
4	Cloud/Virtualization Management Plane	<p>Capture all audit records associated with the management plane for cloud services. This includes, but is not limited to, the following types of actions and information:</p> <ul style="list-style-type: none"> - Management plane authentication, authorization, and access - Configuration changes made - Provisioning of individual services - Changes to the configuration or operation of individual services - System events generated by the management plane - Account management (creation, modification, disablement, deletion) of users, groups, and credentials associated with these objects 	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
5	Cloud/Virtualization Operations	Capture all records related to the use of cloud or virtualization services. These records need to provide sufficient information regarding the details of the operation of the service, and will vary depending on the actual service being consumed. For example, records related to a networking service should include typical information associated with networking such as source, destination, ports, protocols, bytes of data sent and received, etc. whereas a load balancing service likely should include details of HTTP requests and responses to include HTTP verbs, headers, query strings, etc. Audit logs must be captured for any cloud or virtualization services in use.	12 months
6	Container Management Plane	Capture all audit records associated with the management plane for container clusters/pods. This includes, but is not limited to, the following types of actions and information: <ul style="list-style-type: none"> - Management plane authentication, authorization, and access - Configuration changes made - System events generated by the management plane - Account management (creation, modification, disablement, deletion) of users, groups, and credentials associated with these objects 	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
7	Container Operations	Capture all records related to the use of containers. These records need to provide sufficient information regarding the details of the operation of the containers including both the details of the management engine running the containers as well as the events associated with the operating systems within each container (unless EDR has been deployed to the container). Records related to the management engine running the containers should include, at a minimum, container start, stop, crash, errors, resource consumption, and configuration changes.	12 months
8	Identity Management	Capture all records relating to authentication and authorization events including details regarding the creation, modification, disablement, and deletion of users, groups, and other directory/identity services objects. This includes actions taken on credentials associated with objects as well as the objects themselves. Records must include sufficient information to establish the source of the event, time, object being acted on, and outcome (success/failure).	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
9	Authentication and Authorization	Capture all records relating to authentication and authorization events including details regarding account logon, logoff, privilege escalation, and object access attempts. Records must include sufficient information to establish the source of the event, time, object being acted on, and outcome (success/failure).	12 months
10	Email Filtering, Spam, and Phishing	Capture records associated with all inbound email traffic including basic date/time, sender, recipient, subject, and email headers. In addition, each email transaction must include events related to sender validation checks (i.e.- DMARC, SPF, etc. checks), domain reputation checks, spam and malware checks and scoring, and any other outcomes of filtering rules.	12 months
11	Networking	The system must provide event logging for core networking functions that are deployed for ingress/egress traffic such as: routers, switches, firewalls, and reverse proxies. Records must include, at a minimum, sufficient information to determine the source, destination, ports, protocols, request/response bytes transmitted, event or action, alerts or messages generated by the system, outcomes associated with the event (i.e.- blocked, allowed, etc.), and other details necessary to understand the activity. These services/systems are applicable whether deployed in legacy or cloud-based IT environments.	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
12	Application and Database	<p>Capture all records as defined in Identity Management and Authentication and Authorization as they relate specifically to applications and databases. For example, management of users, groups and credentials within a database management system or application needs to be audited and captured. In addition, these systems must capture records of transactions and events specific to these technology layers (i.e., for a database this includes SELECT, INSERT, UPDATE, TRUNCATE, etc. actions), application configuration changes, information regarding the source and destination of the requests associated with the application or database access, outcomes (success, failure, etc.), and errors associated with the database or application.</p>	12 months

	EVENT SOURCE	DESCRIPTION	RETENTION PERIOD
13	Network Security Systems	The system must provide event logging for core security functions that are deployed for ingress/egress traffic such as: Intrusion Detection Systems (IDS), Data Loss Prevention (DLP), dynamic malware prevention systems, Web Application Firewalls (WAFs), and web proxies and content filters. As always, records should include, at a minimum, sufficient information to determine the source, destination, event or action, alerts or messages generated by the system, outcomes associated with the event (i.e.- blocked, allowed, etc.), rule identifier, rule name, and other details necessary to understand the activity. These services/systems are applicable whether deployed in legacy or cloud-based IT environments.	12 months
14	Key Management	Capture all records related to the management of keys used for cryptographic functions including Public Key Infrastructure (PKI) or other Key Management Systems (KMS). This includes key provisioning, revocation, access, expiration, update, recovery, etc. actions with sufficient information to determine the source of the event, object being acted on, date/time of the event, and outcome (success/failure).	12 months