DNP DO NOT PAY

BUREAU OF THE FISCAL SERVICE

Analytics Project Implementation Guide

December 2023

Table of Contents

SECTION 1: Introduction to Do Not Pay Analytics 2
1.1 Do Not Pay Background 2
1.2 Do Not Pay Analytics Services 2
1.3 What Types of Analyses Does DNP Analytics Provide? 3
1.4 What Types of Customers Partner with DNP Analytics? 3
SECTION 2: Death Record Confidence Scoring Tool 4
SECTION 3: Data Sources 6
3.1 Use of Data Sources in Analytics Projects 6
3.2 Federal Customers and State Customers Available Data Sources List Comparison 6
SECTION 4: Project Timeline 8
4.1 How to Request a Project from DNP Analytics 8
4.2 Roles and Responsibilities 8
4.3 Meetings to Expect 9
4.4 Governance Process – Customer Acknowledgement Form 11
4.5 Data Discussion 11
4.5.1. Data Transfer – Secure File Transfer Set-up 11
4.5.2. Data Transfer – Secure File Transfer Testing 12
4.5.3. Data Transfer - Data Specifications 13
4.6 Project Execution 13
4.7 Feedback 14
SECTION 5: Project Governance 15
5.1 Federal Customers – Customer Acknowledgement Form 15
5.2 State Customers – Customer Acknowledgement Form 16
APPENDIX A: Data Source Descriptions 17
APPENDIX B: File Transfer Form 20
APPENDIX C: File Specifications for Analytics Projects 22

SECTION 1: Introduction to Do Not Pay Analytics

1.1 Do Not Pay Background

Do Not Pay (DNP) operates a resource dedicated to assisting federal agencies and federally funded, state-administered programs in preventing and detecting improper payments. DNP's services are no-cost to agencies and state programs. DNP provides centralized access to a variety of relevant data sources for verifying payment and award eligibility through data matching in the DNP Portal. DNP also provides customized data analytics services to help agencies and state programs detect fraud, waste, and abuse.

DNP is authorized and governed by the Payment Integrity Information Act of 2019 (PIIA) and several Office of Management and Budget (OMB) memoranda and circulars. OMB designated the Department of the Treasury to host the Working System to assist federal agencies in identifying and preventing improper payments. The Bureau of the Fiscal Service (Fiscal Service) operates the DNP Business Center.

DNP's goals are to:

- provide timely, accurate, and actionable information about payees and payments to assist customers in identifying, preventing, and stopping improper payments,
- develop and assist customers in implementing cutting-edge techniques to protect the integrity of payments and awards,
- innovate and introduce new tools, technologies, and strategies to support customers in identifying and preventing a wide variety of improper payments.

1.2 Do Not Pay Analytics Services

DNP Analytics, part of the DNP Business Center, provides custom analyses to meet customers' business needs. DNP's analytics services come at no cost to the customer.

DNP conducts analytics projects to:

- identify payees, individuals, and vendors who are ineligible to receive federal and state benefits,
- detect data quality issues and process improvements in areas where internal controls are not effectively preventing improper payments,
- carry out other custom analyses which are tailored to the customer's business problems and business rules.

The DNP Analytics team is comprised of data analysts and data scientists, who are experts in complex analyses and data wrangling. The analytics team includes analytics consultants who serve as liaisons between the customer and the project team to ensure that the analysis conducted is exactly aligned to the customer's expectations. Analytics projects conducted by DNP are centered on a customer's data set. The analytics team uses the customer's data in conjunction with the data sources available to DNP to generate analytics results and report actionable findings.

1.3 What Types of Analyses Does DNP Analytics Provide?

DNP Analytics conducts a variety of projects that are related to the identification of improper payments. Recent projects have included the following types of analyses:

- Vendor and individual eligibility verification
- Deceased payee analysis (including projects using the Death Record Confidence Scoring Tool – see *Death Record Confidence Scoring Tool* section below)
- Data quality and integrity checks
- Business risk assessment
- Payment accuracy
- Vendor consolidation
- Cross-agency analysis
- Ad-hoc analysis and custom analytics research

1.4 What Types of Customers Partner with DNP Analytics?

DNP Analytics conducts analytics projects for the following entities and initiatives:

- Federal agencies
- Federal oversight groups
- Federally funded, state-administered programs
- State oversight groups
- Enterprise customers

SECTION 2: Death Record Confidence Scoring Tool

The Death Record Confidence Scoring Tool (DRC Scoring Tool) is a product developed by DNP to help analytics customers prioritize their research efforts and improve their adjudication processes. The DRC Scoring Tool enables DNP to effectively identity deceased individuals within a dataset, and helps customers understand which payments are most at risk of being issued to a deceased payee. DNP recommends the DRC Scoring Tool for analytics projects focused on identifying decedents within a customer's data. The results are prioritized based on the individuals most likely to be deceased or that have the highest risk based on dollar value. This lets customers know which records to review first.

The DRC Scoring Tool analyzes all death data available to DNP. DNP uses this analysis to determine the accuracy of the death information, and account for difference in data quality between the records. The DRC Scoring Tool converts this information into a confidence score based on the likelihood the individual is truly deceased. DNP then uses the confidence score, in combination with payment information within the customer's dataset, to identify the records that have the greatest potential impact for customers. This helps them reduce the amount of time spent researching and adjudicating records that may have little value.

Benefits of the DRC Scoring Tool:

- ✓ Customers gain a better understanding of which individuals within their data may be deceased based on a confidence score.
- ✓ Potentially improper payments to deceased individuals are uncovered and rank-ordered based on potential impact to the agency.
- ✓ Customers achieve additional assurance of their payment integrity.
- ✓ Customers benefit from less time spent conducting external research, and increased efficiency in their adjudication processes.

Features of the DRC Scoring Tool:

- DRC Scoring Tool provides information to customers in a user-friendly file that helps them ingest, prioritize, and act on the information. The interface has the following key features:
    - payments and the death record matches are grouped together for each payee, rather than listed as individual line items and mixed in with matches against other payees,
    - interactivity to allow users to quickly navigate through the tool and extract information,
    - research priority of each payee based on the likelihood of death, strength of the match, dollars at risk, and how soon the next payment is anticipated,
    - probability of death and the accuracy of the match (death and match confidence),

- estimated disbursement date of the next anticipated payment to aid in determining how urgently adjudicating and potentially stopping the payment should be addressed,
- number and value of at-risk payments,
- date that a second death source listed the individual as deceased.

SECTION 3: Data Sources

3.1 Use of Data Sources in Analytics Projects

DNP's analytics projects use a wide range of data sources to meet customers' needs. The data sources available to DNP include information on death, payment recipient eligibility, debarment, delinquent federal debts, and payment information. DNP leverages the information within these data sources in combination with the data provided by the customer to identify improper payments and other project goals. Many of the data sources available to DNP provide an indication of a payment recipient's eligibility. For example, if a payment recipient was identified on a data source as "deceased," then a payment made to that individual is potentially improper. DNP also uses the information in the available data to conduct a variety of other types of analyses for customers such as business risk assessments, cross-government analysis, and network analysis.

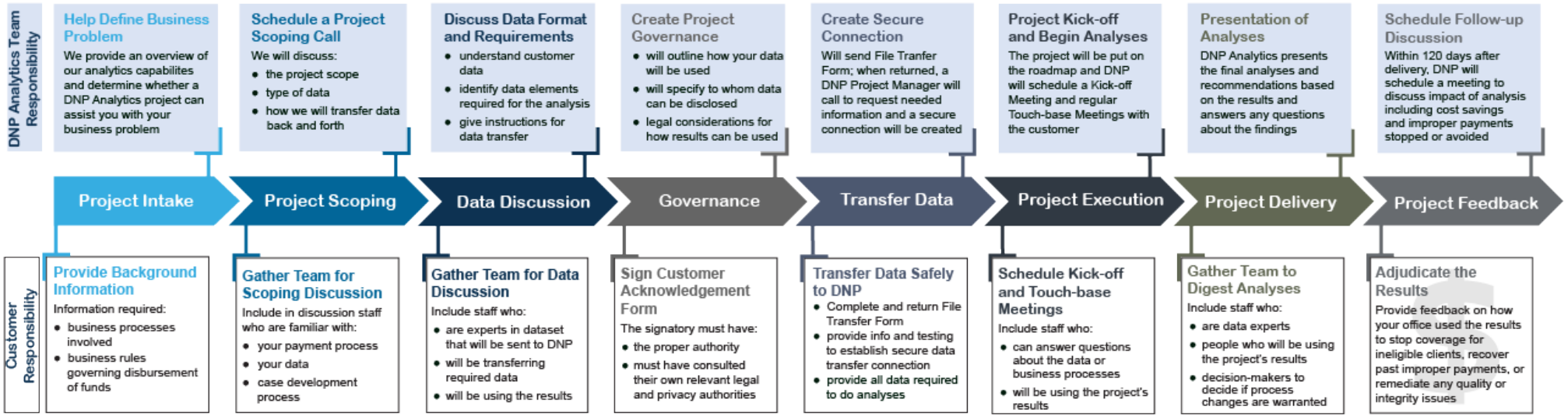
3.2 Federal Customers and State Customers Available Data Sources List Comparison

Below are the data sources currently offered for inclusion in DNP Analytics projects. Federal customers' available data sources are shown with a checkmark in the first checkbox column; state customers are shown in the second checkbox column. (*For a detailed description of each data source, see Appendix A*.)

Data Sources	Available to Federal Customers	Available to State Customers
Death Data Sources		
Death Master File-Full (DMF-Full) *DMF-Full will be available for DNP Analytics in February 2024*	√	√
American InfoSource (AIS) – Probate	√	√
American InfoSource (AIS) – Obituary	√	√
Department of Defense (DoD) Death Data	√	√
Department of State (DoS) Death Data	√	√
Electronic Verification of Vital Events – Fact of Death (EVVE FOD)	√	√
Payments, Claims, and Enhanced Reconciliation (PACER) Death Data	√	

Data Sources	Available to Federal Customers	Available to State Customers
Eligibility Data Sources		
System for Award Management (SAM) Entity Registration Records, Public	√	√
System for Award Management (SAM) Entity Registration Records, Restricted	√	
IRS Tax Exempt Organization Search – Publication 78 (PUB78)	√	√
IRS Tax Exempt Organization Search – Automatic Revocation List (ARL)	√	√
IRS Tax Exempt Organization Search – 990-N (e-Postcard)	√	√
Debarment Data Sources		
System for Award Management (SAM) Exclusion Records, Public	√	√
System for Award Management (SAM) Exclusion Records, Restricted	√	
List of Excluded Individual and Entities (LEIE), Public	√	√
List of Excluded Individual and Entities (LEIE), Restricted	√	√
Office of Foreign Assets Control (OFAC)	√	√
Delinquent Debtor Data Sources		
Treasury Offset Program (TOP) Debt Check, Restricted	√	
Credit Alert System (CAIVRS) - Input from Veterans Affairs (VA)	√	
Credit Alert System (CAIVRS) - Input from Small Business Administration (SBA)	√	√
Credit Alert System (CAIVRS) - Input from Housing and Urban Development (HUD)	√	√
Credit Alert System (CAIVRS) - Input from Department of Justice (DOJ)	√	
Credit Alert System (CAIVRS) - Input from U.S. Department of Agriculture (USDA)	√	√
Payment Data Sources		
Payment Automation Manager (PAM) Payment Data	√	
Payments, Claims, and Enhanced Reconciliation (PACER) Payment Data	√	

SECTION 4: Project Timeline



4.1 How to Request a Project from DNP Analytics

To engage in an analytics project with DNP Analytics, please contact your Agency Lead/Agency Specialist, the Do Not Pay Agency Support Center at 855-837-4391, or email the Do Not Pay Mailbox at donotpay@fiscal.treasury.gov.

4.2 Roles and Responsibilities

Undertaking an analytics project requires committed action from both the customer and DNP. The success of an analytics project depends on the follow-through of DNP and the customer to meet their respective responsibilities. The roles and responsibilities of DNP Analytics during a project engagement include:

- creating the governance form that is required to engage in the requested analyses,
- getting internal legal, privacy, and leadership approval for the form,

- guiding the customer through the data intake and data transfer processes,
- meeting with the customer to discuss any business rule or data questions,
- executing the analysis and delivery of project results,
- following up with the customer to ensure full understanding of the project's results and to address all questions regarding the analyses.

The roles and responsibilities of the customer during a project engagement include:

- providing DNP Analytics comprehensive understanding of the background of the analytics project request as well as any applicable business rules,
- approving the governance form with all applicable internal parties,
- providing required information/testing to establish a secure data transfer connection,
- providing all necessary data to DNP Analytics,
- answering questions from DNP that may arise about the data or business processes while the project team is in execution,
- providing feedback on the final deliverable and project results within 120 days of project delivery.

4.3 Meetings to Expect

Analytics projects include several meetings between the customer and DNP, from project intake to project feedback. Outlined below is a list of the different types of meetings that can occur over the course of an analytics project engagement with DNP.

- **Project Intake:**
  - *Purpose* – to familiarize the project requestor with DNP Analytics, provide an overview of our analytics capabilities, and to determine whether a DNP Analytics project can assist the requestor with their business problem.
  - *Customer participants to include* – personnel who will be using the results, and personnel in a leadership role who will be approving the project under discussion.
- **Project Scoping:**
  - *Purpose* – to further understand the customer's business problems, business rules, and the determine the type of analysis needed.
  - *Customer participants to include* – personnel who will be using the results, personnel in leadership role who will be approving of the project taking place, and data experts.
- **Data Discussion:**
  - *Purpose* – to understand the customer's data that will be used for the analytics project, including any nuances of the data. During this meeting, critical data elements necessary for the analysis are identified and discussed. Additionally, instructions for the data transfer are provided at this meeting.
  - *Customer participants to include* – personnel who are experts in the dataset which will be used, personnel who will be accessing the data transfer connection and

transferring the required data to DNP, and personnel who will be using the results of the analysis.

- **Project Kick-off:**
  - *Purpose* – to allow the analytics team executing the project to ask any initial questions that have arisen during project preparations. This meeting also provides the customer with an idea of the final deliverable.
  - *Customer participants to include* – personnel who will be using the project's results and data experts.
- **Project Touch-bases:**
  - *Purpose* – to meet on a set cadence throughout project execution to verify that the project team is on the right track and to allow the team to ask the customer any questions that may have come up during project execution. The meeting cadence will be set at the beginning of project execution and will be agreed upon between DNP Analytics and the customer.
  - *Customer participants to include* – personnel who will be using the project's results and data experts.
- **Project Delivery:**
  - *Purpose* – to allow DNP Analytics to present the final analysis to the customer and to answer any initial questions that the customer may have about the analysis or its findings.
  - *Customer participants to include* – personnel who will be using the project's results, personnel in a leadership role who may be involved with any business changes as a result of the analysis, and data experts.
- **Project Feedback:**
  - *Purpose* – to allow DNP Analytics to talk to the customer about the project feedback. This discussion may include how the analysis has influenced their business processes, as well as the volume of improper payments that the analysis helped identify and/or stop.
  - *Customer participants to include* – personnel who will be using the project's results.

4.4 Governance Process – Customer Acknowledgement Form

DNP analytics projects must abide by a governance process that is aligned with the privacy and legal considerations associated with matching to and sending a customer's data. A governance form called the Customer Acknowledgement Form is drafted by DNP for each analytics project. A project's governance form serves as a project authorization document and provides specific information about the proposed analytics project including project description, data sources matched to, how the project results and data will be used, and other essential information about the analytics project. The governance form is different for federal partners vs. state partners (see *Governance* section below for examples).

- DNP Governance Signatories:
    - FRB STL Analytics Senior Manager
    - DNP Legal Counsel
    - DNP Privacy Counsel
    - DNP Outreach Manager
    - DNP Director
    - Payment Management Director/other Payment Management signatory (if applicable)
    - CAIVRS/TOP approval (if those data sources are included in the scope of the analytics project)

After the Customer Acknowledgement Form is approved by all applicable internal parties, it is sent to the partnering agency or state for digital signature. The document must be signed by the customer prior to the project starting and data being shared. The agency or state can appoint their own signatory, with the expectation that the individual signing the Acknowledgment Form has proper authority and has consulted relevant legal and privacy authorities within their organization.

4.5 Data Discussion

Before the project commences, DNP Analytics will meet with the partnering organization for a data call to better understand the customer's dataset. During this call, DNP will:

- walk through the steps for setting up a secure data transfer connection,
- give details on file specifications,
- discuss data fields preferred for the analysis.

Any personnel who will be extracting the data and/or transferring the data to DNP, and any data experts who can answer questions about the requested data should be included in this call. Once the Customer Acknowledgement Form has been approved by all DNP signatories and the customer, the customer's dataset may be transferred to DNP.

4.5.1. Data Transfer – Secure File Transfer Set-up

The most common method DNP Analytics uses to receive data and send completed analyses is through a Secure File Transfer Protocol (SFTP) connection. To begin the process of setting up a SFTP connection, the customer will fill out an Analytics File Transfer Form (*see appendix B*).

Once this form is completed and submitted, DNP's Project Manager will contact the partnering organization to request the required information for setting up the SFTP connection. The requested information should not be given through email and needs to be given via a telephone call.

The following information is required for each person who will need access to the SFTP connection:

- Full Name
- IP Address
- Phone Number
- Email Address

For SFTP, the agency will use a client to connect to the Bureau of the Fiscal Service (BFS) SFTP server. If an agency does not already have an internal SFTP client, WinSCP is a free and supported option.

4.5.2. Data Transfer – Secure File Transfer Testing

Once this information is given to DNP's Project Manager, the SFTP connection will be created for the customer. The DNP Project Manager will contact the partnering organization with instructions to test the connection. When sending a test file, put ".TST" or ".TEST" at the end of the file to indicate it is a test file. When sending files to DNP, put them in the Inbound folder. If DNP is sending you files, they will be located in the Outbound folder.

4.5.3. Data Transfer - Data Specifications

Below are the preferred general file specifications for DNP Analytics. See *Appendix C File Specifications for Analytics Projects* for more detailed information. Adhering to these specifications allows for a quicker data loading and cleaning process. However, not being able to provide data in the requested format is not prohibitive to engaging in a project with DNP Analytics.

When submitting data, DNP Analytics requests that partnering organizations:

- submit their data in a CSV Pipe Delimited file,
- do not submit non-ASCII characters,
- prepare and submit a data dictionary with their data file, which includes field names, a definition for each field, the data type of each field, and any other pertinent information about the data file.

The project team needs several days with the data to allow time to load, clean, format, and familiarize themselves with the data. Due to this, data should be sent to DNP at least a week prior to the project execution start date. This date will be communicated to the customer once the Customer Acknowledgement Form is signed by all parties and the project has been scheduled on the DNP Analytics Roadmap.

4.6 Project Execution

Once the Customer Acknowledgement Form has been approved by internal DNP signatories and the customer, the project will be put on DNP's backlog and put on the roadmap for kick-off with the next available project team. DNP Analytics works in an Agile format, which is comprised of two-week sprints. At the project kick-off meeting, DNP Analytics will provide an estimated project completion date based on how many sprints the project is expected to take. This estimate is subject to change. If the estimated time is extended or shortened, DNP will notify the customer of this change.

DNP Analytics will meet with the partnering organization throughout project execution for touch-base meetings to make sure the project is on track and to ask any questions that come up during execution. The customer's data experts who can answer any data-related questions and program personnel who are able to answer questions about business rules related to the program are both helpful participants in these touch-base meetings.

Once the project is completed, the deliverable and results will be uploaded to the SFTP and DNP Analytics will notify the customer when results are available. After the analysis has been received by the partnering organization, DNP will schedule a project delivery meeting to discuss the results of the analysis and answer any questions the customer has.

4.7 Feedback

After project delivery, DNP Analytics requests that the customer provide feedback on the analytics project results and deliverable within 120 days of results delivery. This feedback is critical and enables DNP to improve future analyses and better understand the customer's business processes and rules.

Some key metrics that DNP Analytics would like feedback on include but are not limited to:

- the actual or projected number and dollar amount of improper payments identified and/or prevented,
- costs avoided or projected to be avoided through process improvements or other results of the analytics project (including savings from centralizing processes by the decision to access the DNP Portal),
- other direct or indirect benefits flowing from the project.

The timeframe for providing feedback can be extended by mutual written agreement of DNP and the customer.

SECTION 5: Project Governance

5.1 Federal Customers – Customer Acknowledgement Form

The Customer Acknowledgment Form for federal customers will include:

- a high-level description of the purpose of the work to be carried out
- a description of the project deliverable(s) which will be provided at project completion, including what types of analyses DNP will perform
- a description of the privacy implications related to the project and possible limitations on how the results can be legally used,
- a description of the feedback policy, which states that the customer will provide feedback within 120 days of delivery of the results in order to maintain access to DNP Data Analytic Services,
- a list of all data sources that will be used to match against customer data, and an approval section that spells out any data source agreements discussed with DNP,
- a section that notes the System of Records Notice (SORN) that covers the data that will be in the project engagement
    - For this section to be completed, the customer must provide DNP Analytics with the applicable SORN and routine use that allows for the analytics engagement to be completed.
- an example of this requested information is shown here:

    - *The data that SIGPR will provide to DNP for matching purposes will come from the following two data systems:*
        - *Treasury .015 - General Information Technology Access Account Records*
            - *The data system is covered by system of records notice at: https://www.federalregister.gov/documents/2020/11/17/2020-25298/privacy-act-of-1974-system-of-records*
            - *The following routine use of the SORN applies: To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.*
        - *Treasury .017— Correspondence and Contact Information*
            - *The data system is covered by system of records notice at: https://www.federalregister.gov/documents/2016/11/07/2016-26662/privacy-act-of-1974-systems-of-records*
            - *The following routine use of the SORN applies: To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.*

- the next section will contain a determination from DNP whether a Computer Matching Agreement (CMA) will be required for the engagement; if so, DNP will notify the customer and begin the process of obtaining one.

5.2 State Customers – Customer Acknowledgement Form

The Customer Acknowledgment Form for state customers will include:

- a high-level description of the purpose of the work to be carried out
- a description of the project deliverable(s) which will be provided at project completion, including what types of analyses DNP will perform
- a description of the privacy implications related to the project and possible limitations on how the results can be legally used
- a description of the feedback policy, which states that the customer will provide feedback within 120 days of delivery of the results in order to maintain access to DNP Data Analytic Services
- a list of all data sources that will be used to match against customer data, and an approval section that spells out any data source agreements discussed with DNP
- a Data Governing Statutes section that documents the customer agreement to allow DNP Analytics to use their data for the stated purposes of the engagement
    - For this section to be completed, the customer must provide DNP Analytics with the applicable statutes that cover the data to be used in the engagement.
    - The statute should indicate that the customer has the authority to subpoena and send data to DNP.

- an example of this requested information is shown here:
    - ***Georgia law (O.C.G.A. 50-6-29)***
        - *GA Department of Audits :: Performance Audits: "the state auditor is empowered to conduct hearings, to summon witnesses, to administer oaths, to take the testimony of such witnesses, and to compel the production, inspection, and copying of documentary evidence, including without limitation evidence in electronic form and documentary evidence that is confidential or not available to the general public, at such time and place as he or she may designate for the purpose of investigating and determining the conduct and record of the employees and officials of any department of the state government."*

- the next section will contain a determination from DNP whether a Computer Matching Agreement (CMA) will be required for the engagement; if so, DNP will notify the customer and begin the process of obtaining one.

APPENDIX A: Data Source Descriptions

A.1 Death Data Sources

Data Source	Owner	Description
American InfoSource (AIS) – Commercial	AIS	Contains obituary and probate information on deceased individuals obtained from over 3,000 funeral homes, thousands of newspapers, and county-level probate records
Death Master File-Full (DMF-Full) *DMF-Full will be available for DNP Analytics in February 2024*	SSA	Contains records of deaths reported to the Social Security Administration (SSA). The deaths reported to SSA come from many sources, including family members, funeral homes, financial institutions, postal authorities, state information, and other federal agencies. ***Does contain vital death records from states.***
Department of Defense Death Data – Public	DOD	Contains information on active-duty U.S. military and Reserves regarding confirmed or presumed deaths
Department of State Death Data – Public	DOS	Contains records of American Citizens who are deceased or presumed deceased while abroad, as reported by U.S. embassies or consulates upon its receipt of a foreign death certificate or finding of death by a local competent authority
Electronic Verification of Vital Events Fact of Death (EVVE FOD)	NAPHSIS	Contains information about death certificates contained within the vital records databases of participating states and jurisdictions
Payments, Claims, and Enhanced Reconciliations (PACER)	Fiscal Service	Contains records of payments made on behalf of the federal government and information on any action taken after a payment has been disbursed; this may include offset activities, disputes, or reclamation, and return of funds due to a death

A.2 Eligibility and Debarment Data Sources

Data Source	Owner	Description
IRS Automatic Revocation of Exemption List (ARL) – Public	IRS	Contains entities that have their tax-exempt status automatically revoked under the law because they have not filed Form 990 series returns or notices annually for three consecutive years
Publication 78 (PUB78) - Public	IRS	Lists of organizations that can receive tax-deductible contributions; • Users may rely on this list in determining deductibility of their contributions. • If an organization uses a "doing business as" (DBA) name, that name will not be listed in the Pub. 78 Data. Only the organization's official name submitted to the IRS is included in the data set. Some donees (i.e., churches, group ruling subordinates, and governmental units) eligible to receive tax-deductible charitable contributions may not be listed in Pub. 78 Data. For more information see, Other Eligible Donees
990-N (e-Postcard) - Public	IRS	Form 990-N 9 (e-Postcard) is an annual electronic notice most small tax-exempt organizations (annual gross receipts normally $50,000 or less) are eligible to file instead or Form 990 or Form 990-EZ
List of Excluded Individuals and Entities (LEIE) – Public & Restricted	HHS OIG	Contains information regarding individuals and entities currently excluded from participation in Medicare, Medicaid, and all other federal health care programs
Office of Foreign Assets Control (OFAC) – Public	Treasury	Contains a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries; it also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific; collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs"; their assets are blocked, and U.S. persons are generally prohibited from doing business with them

Data Source	Owner	Description
System for Award Management (SAM) Entity Registration Records – Restricted	GSA	Contains entity registration data publicly available under the Freedom of Information Act for those entities registered in SAM to do business with the federal government in accordance with the Federal Acquisitions Regulation (FAR)
SAM Exclusion Records – Public & Restricted	GSA	Contains the data for all active exclusion records entered by the federal government identifying those parties excluded from receiving federal contracts, certain subcontracts, and federal financial and non-financial assistance and benefits

A.3 Delinquent Debtor Data Sources

Data Source	Owner	Description
Credit Alert System (CAIVRS) – Restricted	DOJ, HUD, SBA, USDA & VA	Contains information on loan applicants that have any federal debt that is currently in default or foreclosure or has had a claim paid by the reporting agency within the last three years; Although CAIVRS may not identify all federal "delinquent debt" or "prior losses," it is a valuable resource for "delinquent debt"
Treasury Offset Program (TOP) Debt Check – Restricted	Treasury	Contains data on individuals who are delinquent on non-tax debts and child support obligations to the federal government (and participating states) if allowed by agency statute and regulations

A.4 Payment Data Sources

Data Source	Owner	Description
Payments, Claims, and Enhanced Reconciliations (PACER)	Fiscal Service	Contains records of payments made on behalf of the federal government and information on any action taken after a payment has been disbursed; this may include offset activities, disputes, or reclamation, and return of funds due to a death
Payment Automation Manager (PAM)	Fiscal Service	Contains records of ACH, check, and wire disbursements to entities that were made through the Payment Automation Manager payment processing system

APPENDIX B: File Transfer Form

File Transfer Form

Section 1- Access/Contact Identification	
Agency Name:	Agency Acronym:
Technical Contact Name:	Technical Contact Email:
Technical Contact Phone:	Email for Notifications:

Section 2 – File Identification
File Name:
File Description (Application Destination):
Data Submittal Frequency: ☐ Weekly ☐ Monthly ☐ One-Time ☐ Other
How will you securely send us your file? ☐ Connect Direct (Requires additional forms) ☐ SFTP ☐ HTTPS (MoveIT)
How will you connect? ☐ Internet ☐ VPN Tunnel (Additional forms required)
Agency will connect to BFS SFTP server for send/receive, 166.123.219.4 Your Public IP Address: Requested Userid: ----------
Have you reviewed the Naming Convention Standards Document? ☒ Yes ☐ No ☐ NA
Can you comply with the Naming Convention Standards? ☒ Yes ☐ No ☐ NA
File Format: ☐ Mainframe ☐ .txt ☐ xml ☒ csv ☐ compressed type:
Additional Notes About the File:

SFTP (SSH File Transfer Program)

SFTP is widely available for a number of platforms and it solves the problems of securing the user's password and provides data encryption and integrity on the fly. SSH (which SFTP uses as an authentication and data transport mechanism) also authenticates the server involved though the exchange of keys. SSH keys are privately maintained and require external acceptance upon first use or prior transfer through an alternate method.

File Upload Using HTTPS

File Upload Using HTTPS provides the ability to transfer files from your browser and remote Secure HTTP (HTTPS) server.

File Transfer Using Connect:Direct

Connect:Direct is a computer software product to transfer files between mainframe computers, and midrange computers. It was developed for mainframes, with other platforms being added as the product grew. Originally called Network Data Mover (NDM), it was renamed to Connect:Direct by its owner Sterling Commerce in 2008, after Sterling Software purchased the company. In 2010, IBM completed the purchase of Sterling Commerce.

Please note: The HTTPS option, MoveIT, is not available for secure file transmission as of June 2023.

APPENDIX C: File Specifications for Analytics Projects

Preferred File Extensions

- .csv
- .txt
- .txt.gpg
- .gz
- .gpg

Accepted File Formats

- Plain text
- Encrypted plain text
- Encrypted compressed plain text file

Accepted File Delimiters

- CSV
- Tab
- Pipe

Common Issues that will Cause File Problems

- Double delimiters
- Delimiters within field values, or delimiters that are in an unquoted text field

  Example of quoted file sample record: 12.50 | 1122334455 | "ANTHONY MARTIN | AKA TONY MARTIN"

  Load result would be 3 columns as shown below, including the Column Type in parentheses
  Column 1 = 12.50 (Numeric)
  Column 2 = 1122334455 (Numeric)
  Column 3 = ANTHONY MARTIN | AKA TONY MARTIN (Text)

  Example of unquoted file sample record: 12.50 | 1122334455 | ANTHONY MARTIN | AKA TONY MARTIN

  Load result would be 4 columns as shown below:
  Column 1 = 12.50 (Numeric)
  Column 2 = 1122334455 (Numeric)
  Column 3 = ANTHONY MARTIN (Text)
  Column 4 = AKA TONY MARTIN (Text)

- Any delimiter with more than one character column (e.g., "~*")
- Leading zeros dropped when importing into Excel
- Numbers being converted to scientific notation in field values
- Double quotes inside of double quoted fields
- Non-printing characters or non-ASCII characters/symbols in the dataset