

Public Voter File Acquisition and Handling

1 Purpose

The purpose of this acquisition is for the handling and secure delivery of publicly available voter registration files and voter history files to support Homeland Security Investigations (HSI) fraud detection and data segmentation activities.

2 Scope

The Contractor shall acquire, document, and securely deliver public voter registration files and, when applicable, public voter history files from Government-identified U.S. jurisdictions. The Contractor shall also provide technical support on jurisdiction-specific file structures, formats, and fields, as directed by the Government.

For purposes of this section, “jurisdiction” means any U.S. state, the District of Columbia, any U.S. territory, or any other U.S. jurisdiction identified in writing by the Government.

3 Requirements

a. Annual Public Voter File Acquisition

The Contractor shall acquire one public voter registration file from each Government-identified jurisdiction per year, when directed by the Government under the applicable contract line item.

The Government will provide the final list of jurisdictions in writing for each acquisition. The list is anticipated initially to be a limited number of jurisdictions but may be adjusted at the Government’s discretion within the contract ceiling. The Contractor shall have the capability to support acquisition for up to all fifty (50) states, the District of Columbia, U.S. territories, and other U.S. jurisdictions identified in writing by the Government, subject to the contract ceiling and applicable ordering procedures.

The Contractor shall acquire public voter registration files consistent with applicable jurisdictional laws and access procedures.

b. Public Voter History File Acquisition

For each Government-identified jurisdiction, the Contractor shall acquire public voter history files when such files are publicly available and separate from the public voter registration file.

The Contractor shall acquire voter history files for each federal election specified by the Government, including general, primary, runoff, and special federal elections, as applicable and as available under jurisdictional law and access procedures.

If a jurisdiction does not maintain, publish, or make available a separate public voter history file, the Contractor shall document that determination, including the source of the information, date of inquiry, and any applicable jurisdictional response.

c. Timing

The Contractor shall initiate acquisition requests within [X] business days of Government direction unless otherwise approved by the Contracting Officer.

The Contractor shall deliver acquired files to the Government within [X] business days after receipt and completion of required integrity checks, unless otherwise directed by the Government.

d. Consolidated Acquisition and Delivery

The Contractor shall not prioritize, delay, sequence acquisition, or deliver files based on political characteristics of any jurisdiction or electorate. Sequencing shall be based solely on operational, technical, legal, or schedule considerations as directed by the Government.

e. Deliverables

The Contractor shall provide the following deliverables, as applicable:

1. Public voter registration file for each Government-identified jurisdiction.
2. Public voter history file for each Government-specified federal election, when publicly available and separate from the public voter registration file.
3. Chain of custody documentation for each acquired file.
4. File integrity documentation, including cryptographic hash values.
5. Technical documentation describing file format, field names, field definitions, and known anomalies or limitations.
6. Documentation of unavailable files, denied requests, statutory limitations, jurisdiction-specific access restrictions, or other issues affecting acquisition or delivery.

f. Secure Electronic Delivery

The Contractor shall deliver all files to HSI via secure electronic means approved by the Government, such as an approved secure file transfer mechanism.

The Contractor shall ensure files are encrypted in transit and, if required by the Government, at rest, using Government-approved encryption.

The Contractor shall transmit associated chain of custody documentation with each delivery.

g. Technical Documentation and Clarification

With each deliverable, the Contractor shall provide documentation describing the file format, field names, field definitions, and any known anomalies or limitations.

Upon Government request, the Contractor shall answer clarifying questions related to the delivered file formats and structures.

The Contractor shall respond to Government inquiries related to file formats and structures within [X] business days, or as otherwise specified by the Contracting Officer.

h. Chain of Custody and Data Handling

The Contractor shall establish and maintain a documented chain of custody for all acquired files, to include at a minimum:

1. Date and method of each request submitted to a jurisdiction or authorized provider.
2. Date, method, and source of each file received.
3. File integrity information, such as cryptographic hash values, applied upon receipt and prior to delivery.
4. Any transformations, conversions, or processing steps performed prior to delivery.
5. Date and method of delivery to the Government.

The Contractor shall ensure chain of custody is preserved from initial acquisition through final delivery to HSI and shall provide chain of custody documentation to the Government upon request and with each delivery.

The Contractor shall handle and store all files in accordance with contract security requirements and applicable DHS policies.

i. Neutrality and Party Affiliation

The Contractor shall not perform any activities under this task that involve political affiliation-based targeting, prioritization, or ranking of jurisdictions or individuals.

The Contractor shall not collect, process, or deliver party affiliation data fields, even if present in jurisdiction-provided voter files, unless explicitly directed in writing by the Contracting Officer.

The Contractor shall perform acquisition and delivery activities in a neutral manner consistent with Government direction and solely in support of the defined fraud detection mission.

Removing Party Data (Without Breaking Chain of Custody). The Dual-Hash "Parent-Child" Protocol:

- a. Parent Hash: The vendor acquires the raw file from the state and immediately generates a cryptographic hash (Hash A) to verify the file was not altered in transit from the source.

- b. Documented Cleansing: The vendor runs an automated, auditable script that strictly strips the prohibited party affiliation fields.
- c. Child Hash: The vendor immediately generates a new hash (Hash B) on the sanitized file.
- d. Verification: The vendor delivers the sanitized file along with a Chain of Custody log containing both Hash A (proving source integrity) and Hash B (proving sanitization integrity). This maintains a legally defensible audit trail.

j. Security and Integrity Controls

The Contractor shall implement access control measures consistent with DHS and contract security requirements, including role-based access controls and strong authentication mechanisms for any systems used to store or process public voter registration files or public voter history files.

The Contractor shall ensure all transmissions of voter files and related documentation to the Government use secure, encrypted protocols approved by the Government.

The Contractor shall maintain audit logs for all access to and handling of voter files, including acquisition, storage, processing, and delivery activities. These logs shall be retained for not less than [X] years and provided to the Government upon request.

The Contractor shall apply integrity verification measures, such as cryptographic hash values or digital signatures, to verify that files have not been altered between acquisition and delivery. Hash values shall be recorded in the chain of custody documentation.

The Contractor's security and integrity controls should be consistent with generally accepted best practices and relevant guidance from recognized bodies, as applicable and as directed by the Government.

k. Navigating Legal Access (State Restrictions)

Where state laws restrict commercial data access but allow law enforcement use, DHS will provide official "Government Interest" / "Need-to-Know" authorization letters to the state on behalf of the contractor. This allows the vendor to act as our designated acquisition agent, clearing the legal hurdle while maintaining the commercial contract structure.