# ERIC: Technology and Security Overview

The Electronic Registration Information Center (ERIC) is a non-profit organization with the sole mission of assisting states to improve the accuracy and efficiency of state voter registration processes. Formed in 2012, ERIC provides sophisticated data matching services to the member states in order to improve a state's ability to identify inaccurate and out-of-date voter registration records, as well as eligible, but unregistered residents. States can then contact the voters, compliant with federal regulation, to encourage individuals to register or update their existing registration. ERIC is owned, governed, and funded by state election officials.

ERIC is dedicated to the highest standards of security and protection of personally identifiable information. The ERIC Board of Directors has appointed a Privacy and Technology Advisory Board, comprised of leading experts in the field of data security and encryption, to review security protections and help provide advice. As of March 2015, the Advisory Board members are:

- Joseph Lorenzo Hall, Chief Technologist at the Center for Democracy and Technology, https://cdt.org/staff/joseph-lorenzo-hall/; and
- Glenn Newkirk, President of InfoSENTRY Services, Inc., http://www.infosentry.com/; and
- Rebecca Wright, Professor of Computer Science at Rutgers University and Director of the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), http://www.cs.rutgers.edu/~rwright1/; and
- Jeff Jonas, IBM Fellow and Chief Scientist in Entity Analytics, http://www-03.ibm.com/press/us/en/biography/40087.wss.

The Advisory Board will continue to review ERIC's technical and governance systems and make recommendations related to security practices.

ERIC takes extraordinary care to keep citizen's information secure while still offering a robust and comprehensive data matching system. The data center was designed by engineers and information security experts from IBM with support from the Pew Charitable Trusts, and is powered by IBM's InfoSphere™ Sensemaking software. The participating states oversee the data center's administration, including technical relationships, operating costs, and routine maintenance. You can find more details about InfoSphere™ here: https://www-304.ibm.com/industries/publicsector/fileserve?contentid=235174

There are three primary components to ERIC's data matching process from the states' perspective: data collection, anonymization, and file transfer. To participate, states must submit their voter registration and license/identification records (other official state data sources may be accepted but are not required) as an ASCII file formatted into XML for the data feed. States are required to provide fields related to name, address, driver's license or state ID number, last four digits of social security number, date of birth, and activity date. As available, states also submit information on current record status, phone number, and email address. To ensure sensitive information is protected and that ERIC does not receive that information in clear text, ERIC provides an anonymization application to each participating jurisdiction for protected fields in the XML. All private data is protected at the source—the state—prior to submission to the ERIC data center. The state election officials can run this application on both the voter rolls and the driver license files or the application may be given to the agency providing license and state ID information (typically, this is the state motor vehicle agency) to be run prior to providing information to the state election officials. States are then given account credentials to access an sFTP site where their anonymized files are uploaded to a state-specific location.

ERIC then runs reports, identifying records that may be outdated or inaccurate and flagging residents who appear to be eligible but have not yet registered. Once the reports are generated, they are available for state-

specific download on the same sFTP site. ERIC employs a full-time systems engineer and technology adviser to guide states throughout the upload and data matching process.

All data run through ERIC is collected, matched, and stored in an environment with state-of-art security protections. ERIC's technical and governing models have been reviewed and commended by leading advocates in the fields of data security and privacy. The anonymization (or "one-way hashing") ERIC uses to protect the privacy of personally identifiable information converts information into an indecipherable string of characters so it is unreadable and unusable to potential hackers. To further strengthen the security measures around the data, all records are sent through the anonymization process twice—once at the state level, before the data is ever sent to ERIC, and once by ERIC as it receives the data. The Center for Democracy and Technology reviewed plans for ERIC and determined that it would improve the quality of voter registration data at the same time as it protects, and even improves, the privacy and security of information shared across state lines for registration purposes. ERIC also maintains audit logs that track activity conducted in the system, including data imports and reports. In addition, all ERIC states are obligated to stringent information security commitments through ERIC's by-laws.