ERIC: Technology and Security Overview

The Electronic Registration Information Center (ERIC) is a non-profit membership organization whose mission is to help state and local election officials improve the accuracy of their voter rolls, register more eligible citizens to vote, reduce costs, and improve the voting process. Formed in 2012, ERIC provides sophisticated data matching services to members in order to improve their ability to identify inaccurate and out-of-date voter registration records, as well as likely eligible, but unregistered residents. Members can then contact voters, in compliance with federal and state regulations, to encourage individuals to register or update their existing registration. ERIC is governed and funded by its members.

Privacy and Technology Advisory Board

ERIC is dedicated to the security and protection of the data in its care. The ERIC Board of Directors appointed a Privacy and Technology Advisory Board, comprised of experts in the field of data security and encryption, to review security protections and provide advice. This board reviews ERIC's technical and governance systems and makes recommendations related to security practices. As of March 2020, the Advisory Board members are:

- Jeff Jonas, Senzing Founder and CEO, https://senzing.com/jeff-jonas-bio/.
- Glenn Newkirk, President of InfoSENTRY Services, Inc., http://www.infosentry.com/
- Rebecca Wright, Professor of Computer Science, Barnard College, and Director, Vagelos Computational Science Center. https://www.cs.columbia.edu/~rwright/

Information Security Management Approach

Information security management, corporate transparency, and oversight are core principles for ERIC. In support of these principles, ERIC employs risk management and information security management techniques that align with industry guidelines published by national and international information security management organizations. ERIC practices include, but are not limited to:

1. Building a culture of continuous review and improvement
2. Using standards-based risk assessment and risk management practices
3. Performing routine internal and external audits of risk profiles and security management policies, operations, and procedures
4. Providing governing board members with scheduled security updates and reviews, consistent with standard corporate transparency guidelines for governance and oversight
5. Requiring members to follow stringent information security commitments via ERIC's by-laws and membership agreement
6. Requiring that its data center vendor provide documentation of an annual security assessment by an independent third party to ensure that their security aligns with industry-accepted standards.

ERIC Operations

As a practical matter, ERIC does not publicly discuss specific security measures. All procedures and software are routinely reexamined during internal risk assessments and security reviews, evaluated by the Privacy and Technology Advisory Board, and addressed in external auditing processes.

Participating as a member in ERIC involves three routine actions: preparing and protecting voter registration and license/identification data, securely transmitting data to ERIC, and securely accessing reports. ERIC employs a full-time Systems Engineer and Technical Liaison to guide members through these processes.

Members provide their voter registration records and license/identification records (other official state data sources may be accepted but are not required). 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 are required, if present. Members also submit information on current record status, phone number, and email address when available.

ERIC distributes to each participating jurisdiction an application that applies a cryptographic one-way hash to sensitive data elements before the jurisdiction submits the data to ERIC. The hashed elements are driver's license or state ID number, any part of the social security number, and date of birth. The hashing application converts the information into what appears to be a string of random characters, making the data significantly more difficult for a potential hacker to utilize. ERIC only accepts voter and driver's license data files that have been hashed using this application. This ensures these sensitive data are protected at the source, in the member's environment, prior to submission to the ERIC data center. A cryptographic hash is not meant to be decrypted so ERIC does not receive this information in clear text and does not restore it to the original values. To further strengthen the security around these data, all records are run through a second hashing process using different parameters once inside the ERIC environment. ERIC uses a hashing module provided by IBM, in conjunction with Senzing (www.senzing.com), which implements an HMAC-SHA2-256 one-way hashing algorithm with a 1024-bit secret key. The secret key is housed in a PKCS#11 interfaced secure store that leverages AES-128 encryption.[i] The distribution of the hashing application to the ERIC members is a closely monitored and structured process.

Once the data file is hashed, ERIC members employ layers of industry-standard security mechanisms to transmit the data to the ERIC data center, including multiple rounds and types of encryption. There are also specific procedures directed at communication of member credentials.

At the ERIC data center, the provided data is processed through a sophisticated matching engine produced by IBM and Senzing. The engine compares common identifying data elements and additional tools such as a name variation database, fuzzy date matching, and record linkage. Record linkage is a matching methodology that compares multiple data sources at the same time. For instance, the mailing address on a DMV record might provide the missing link that confirms a match between two voter records that otherwise wouldn't have enough information on their own be sure. ERIC produces reports for each member by analyzing the results of the matching to identify voter records from that member that may be outdated or inaccurate or people who are not currently registered to vote. Once the reports are generated they are available for secure download. Members cannot access the reports of other members.

Assessment and Review

The Center for Democracy and Technology (CDT) reviewed plans for ERIC in 2011 and determined that ERIC would improve the quality of voter registration data while protecting, and even improving, the privacy and security of information shared across state lines for registration purposes. (The CDT and ERIC are not affiliated.)

ERIC subscribes to the Social Security Limited Access Death Master File in order to provide information on possibly deceased voters to its members. The National Technical Information Service requires subscribers to attain a third-party attestation that its systems, facilities, and procedures adequately safeguard this information. This process must be conducted every three years. It is similar to an audit and includes an extensive review and examination of all information security policies, practices, systems, facilities, and procedures relative to the handling of Social Security data. ERIC successfully received this attestation in 2017 and 2020.

In 2020, ERIC contracted with an independent U.S.-based cyber security firm to conduct a comprehensive assessment of its information security and compliance posture. The external evaluation included the following:

- Cyber security risk assessment using ISO 27001 and 27002 security controls
- Code review of the cryptographic hashing tool used by members and ERIC to secure sensitive data
- Office and network scan and penetration testing.

- Email security assessment
- Phishing/Social Engineering campaign
- Data handling practices relative to member data

The cyber security firm concluded “ERIC has strong data security practices” and identified “no critical findings.”

[i] For more information on the hashing mechanism and secure store, visit https://senzing.zendesk.com/hc/en-us/articles/360000970834-Selective-Feature-Hashing. A free Zendesk account may be required for access.