Electronic Registration Information Center (ERIC): Technology and Security Overview

Introduction

ERIC is a public charity non-profit membership organization comprised of states who choose to join. Formed in 2012, ERIC's mission is to help states improve the accuracy of America's voter rolls, increase access to voter registration for all eligible citizens, reduce election costs, and increase efficiencies in elections. ERIC is governed and funded by its members.

Members securely submit voter registration and motor vehicle department (MVD) data to ERIC. ERIC is also certified to use official death data from the Social Security Administration and subscribes to official change of address data from the United States Postal Service. Utilizing these four data sources, ERIC provides its members with reports that identify inaccurate or out-of-date voter registration records, deceased voters, individuals who appear to be eligible to vote but who are not yet registered, and possible cases of illegal voting. In compliance with federal and state laws, members use these reports to contact voters for the purposes of updating their record or to remove ineligible and deceased voters from the rolls. Members also contact likely eligible but not yet registered individuals, providing information on how best to register. Possible cases of illegal voting are reviewed and, if found credible, referred to law enforcement.

Information Security Management Approach

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

- Building a culture of continuous review and improvement.
- Using standards-based risk assessment and risk management practices.
- Performing routine internal and external audits of risk profiles and security management policies, operations, and procedures.
- Requiring governing board approval of updates to ERIC's Information Security Management Plan, risk assessment, and associated information security policies.
- Requiring members to adhere to information security commitments via ERIC's by-laws and membership agreement, which are consistent with applicable federal laws and regulations.
- Requiring that its data center vendor provide documentation of an annual security assessment by an independent third party to ensure its security practices align with industry-accepted standards.

Information Security Basics

This section provides a general overview of the organization's information security basics pertaining to ERIC Servers and Employees.

ERIC Servers

- For security reasons, ERIC does not publicly disclose the location of the secure U.S. based data center where its servers are housed.
- The data center is hosted by a U.S. based vendor. The vendor is subject to SOC 1 Type 2 and SOC 2 Type 2 audits.
- There is no web-based access to the ERIC servers. ERIC's website is not connected to or hosted on the servers.
- Member do not have access to any other member's data or reports stored on the servers.
- ERIC servers are never connected to any state's voter registration system.
- Only authorized ERIC employees have access to the ERIC servers. Members and Advisory Board Members do not have access to the servers.

ERIC Employees

- Employees must pass a criminal background check.
- Employees must sign an agreement to comply with ERIC's information security policies, procedures, and practices.
- Employees work remotely from U.S. based locations. Secure remote access to the data center is limited to only employees who need it to perform their duties.

Data Security in Practice

Participating as a member in ERIC involves preparing and securely transmitting data to ERIC, and securely accessing the reports ERIC generates.

Preparing and Securely Transmitting Data

At least every 60 days, each member submits their voter registration data and licensing and identification data from their MVD to ERIC. ERIC refers to these data as Member Data. Data 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 (e.g., is the record "active" or "cancelled"), phone number, and email address when available. These fields improve the quality of the data matching process.

ERIC distributes to each member an application that applies a cryptographic one-way hash to sensitive data elements before the jurisdiction submits the data to ERIC. The ERIC hashing application uses a module provided by IBM, in conjunction with Senzing, 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.[ii]

The sensitive data elements are the driver's license or state ID number, any part of the social security number, and date of birth. The hashing application converts these data into what appears to be a string of random characters, making the data significantly more difficult for a potential hacker to utilize. A cryptographic hash is not meant to be decrypted. ERIC only accepts voter and driver's license data files that have been hashed using the application. This ensures these sensitive data are protected at the

source, in the member's environment, prior to submission to the ERIC data center. The distribution of the hashing application to ERIC members is a closely monitored and structured process.

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

ERIC Data Management, Matching, and Report Delivery

Once ERIC accepts the data files, ERIC applies the hashing process to the same sensitive data elements a second time using different hashing parameters. This ensures the hashed values are different and more secure.

At the ERIC data center, the Member Data and official death data from the Social Security Administration are combined using data matching software developed by Senzing and licensed through IBM. The data matching software[iii] compares common fields like name, address and other identifiers to determine if the records are about the same people. Entity-centric learning is used to match smarter as more records become available. 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 to 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. (Visit www.ericstates.org for more information on the reports ERIC produces for its members.)

External Assessment and Review

As a matter of best practice and in support of the organization's mindset of continuous improvement, ERIC subjects itself to independent review of its information security practices, policies, procedures, and systems. These independent assessments are in addition to ERIC's annual internal review of its Risk/Threat Assessment, Information Security Management Plan, and associated policies and procedures.

To maintain its subscription to the Social Security Limited Access Death Master File, ERIC complies with the National Technical Information Service subscriber requirement 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. ERIC will again complete this required third-party attestation in 2023.

In 2021, ERIC utilized information security assessment services from the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). These included a cyber-hygiene review and an External Dependencies Assessment. At no time during these engagements did DHS or CISA have access to ERIC's servers, data, or technical infrastructure.

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 hashing application 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."

ERIC Board of Directors and Privacy and Technology Advisory Board

The ERIC Board of Directors is dedicated to the security and protection of the data ERIC utilizes, the reports it provides members, and the organization's critical infrastructure. The Board of Directors reviews and approves annual updates to ERIC's Information Security Management Plan, Risk/Threat Assessment, and associated policies and procedures. The Board also provides advice and guidance on external assessments, and reviews external assessment reports.

Upon ERIC's founding in 2012, the Board appointed a Privacy and Technology Advisory Board to advise on best practices and support the organization's "continuous improvement" mindset toward data security and privacy. The advisory board is comprised of up to four experts in the field of data security, data matching, and encryption and has no governing authority. The advisory board reviews ERIC's Information Security Management Plan and makes recommendations related to security and data handling practices. It does not have access to the data ERIC utilizes or to ERIC's technical infrastructure. Advisory Board members:

- 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/

[i] Review ERIC's Membership Agreement for more information on the legal protections that apply to the data ERIC utilizes and the reports it generates for its members.

[ii] 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.

[iii] The technical term is "Entity Resolution." Simply put, Entity Resolution is the process of determining when real world entities are the same, despite differences in how they are described. For example, a voter registration record and a DMV record that have the same name and address, but the dates of birth clearly indicate it is a junior and senior; not the same person. For more on Entity Resolution watch this explainer video: https://senzing.com/what-is-entity-resolution/