Request for Proposals (RFP)

RFP Topic: Information Security Assessment

Issuance Date: April 8, 2019

Deadline for Letter of Intent and Questions: April 22, 2019

Deadline for Proposals: May 20, 2019

Point of Contact: Shane Hamlin, shane.hamlin@ericstates.org

Table of Contents

PURPOSE

The purpose of this RFP is to solicit proposals from firms (BIDDERS) qualified to perform an information security assessment of the Electronic Registration Information Center's (ERIC) Information Security Management System (ISMS). The assessment will include, at a minimum, an evaluation of ERIC's security policies and procedures to ISO 27001 and ISO 27002, specific security-related testing, and an overall review of ERIC security and sensitive data handling practices. The selected BIDDER will review, assess, evaluate and make recommendations for improvement of security-related services procured, deployed, maintained, and operated by ERIC.

ERIC will consider proposals from single BIDDERs or from multiple BIDDERs working as a team. The ideal BIDDER(s) will have experience assessing ISMS for small organizations operating in multiple locations.

BACKGROUND

ERIC is a 501(c)(3) not-for-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sophisticated data matching services to its members in order to improve their ability to identify inaccurate and out-of-date voter registration records, as well as likely eligible, but unregistered residents.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 laws, to provide information on how to register or update their existing registration. ERIC is governed and funded by the member jurisdictions.

As of April 1, 2019, 25 states and the District of Columbia are members:

Alabama	Illinois	Minnesota	Oregon	Virginia
Alaska	Iowa	Missouri	Pennsylvania	Washington
Arizona	Louisiana	Nevada	Rhode Island	Washington D.C.
Colorado	Maryland	New Mexico	South Carolina	West Virginia
Connecticut	Michigan	Ohio	Utah	Wisconsin
Delaware				

Since its inception, ERIC has placed a primary emphasis on the security of the information assets in its control, including Social Security death data, voter registration-related data, and driver's licensing data, of which the latter two are submitted to ERIC by its members on a routine basis. The secure transmission and storage of these data is fundamental to ERIC's operational posture. ERIC is acutely aware that its information systems and networks will generate, possess, process, and transmit substantial quantities of data, some of which will contain personally identifiable information (PII).

ERIC has developed an ISMS based on the guidelines in:

- ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management
- Center for Internet Security Controls

ERIC does not specifically adhere to all the standards and guidelines listed in the above. However, ERIC has incorporated many of the frameworks and concepts in these standards and controls into its ISMS and data protection strategy. ERIC will gladly consider specific recommendations from the selected BIDDER, based on these standards and guidelines, that will (1) improve ERIC's management of risks and threats to its information

security assets and processes, particularly its data and databases, and (2) provide value-added benefit to ERIC's members.

In 2017, ERIC received a third-party attestation that it adequately safeguards Social Security data in compliance with federal data handling standards. This process included an extensive review and examination of ERIC's ISMS relative only to the handling of Social Security data.

ERIC's website, www.ericstates.org, provides substantive background information about ERIC's governance structure, strategic direction, organization, information assets, and data management operations.

SCOPE OF WORK

The selected BIDDER will be required to gather information through facilitated meetings with ERIC staff, and other resources determined in the approved work plan between ERIC and the selected BIDDER. Deliverables will include but may not be limited to a methodology or approach, development of schedule and meetings, and threat and vulnerability assessment reports.

Components of the information security assessment:

1. Review ERIC's policies and procedures for:
    a. Alignment to ISO 27001 and ISO 27002
    b. Comprehensiveness and effectiveness
    c. Staff compliance to ERIC policies and procedures
2. Vulnerability scan: scan the specified systems and report possible vulnerabilities and what steps are necessary to mitigate them:
    a. Scans of staff office environments
    b. Review of data center vendor-provided vulnerability scan reports of VPN
    c. Review of data center vendor-provided vulnerability scan reports of sFTP service
3. Penetration testing: attempt to gain access to the specified environments with permission from ERIC management:
    a. Testing of staff office environments
    b. Review of data center vendor-provided penetration test reports of VPN
    c. Review of data center vendor-provided penetration test reports of sFTP service
4. Social engineering testing: use remote engagement techniques, such as a managed phishing campaign, to assess ERIC staff security awareness with permission from ERIC management.
5. Email assessment: assess email system configuration to evaluate email security and potential exposure to malicious payloads sent by email.
6. Code analysis of hashing application:
   ERIC provides an application to member states to apply a one-way cryptographic hash to the sensitive data elements of date of birth, driver's license number, and last four digits of the social security number before sending information to ERIC. Review 1,000 lines of code for potential vulnerabilities and make recommendations for mitigation.
7. Overall security and sensitive data handling practices:
   Review ERIC's overall approach, implementation, and application of risk and information security management for potential risks and vulnerabilities, and make recommendations for improvements or mitigations. Review will include, at a minimum:
    a. Risk and security management plan and practices
    b. Sensitive data flow
        i. State data

        ii. Social Security Death Master data
        iii. United States Postal Service National Change of Address data
    c. Vulnerability reporting and incident handling processes
    d. System architecture
        i. Network
        ii. Configuration
        iii. Remote access to data center
    e. Data center vendor SOC I and SOC II audit reports for applicability and completeness as related to ERIC operations and ISMS
    f. Staff office environments
        i. Endpoint security evaluation
        ii. Physical security
        iii. Equipment
        iv. Network
        v. Configuration
        vi. User procedures and habits
    g. Credentialing review
        i. ERIC staff
        ii. sFTP logins provided to ERIC member staff

Additional assessment topics proposed by the selected BIDDER will be considered.

EXCLUSIONS

1. Review of the data center architecture, configuration, and data center vendor procedures and practices will be limited to review of the SOC I and II audit reports, and staff interviews, if necessary. Additional assessment or testing of the data center itself may be recommended in the final report, but will not be performed as part of this body of work.
2. The selected BIDDER will not be asked to implement corrective measures for any system deficiencies or vulnerabilities as part of this body of work.
3. The ERIC website will not be included in this assessment.

DELIVERABLES

1. Project management
    a. Project schedule within one week of project start date
    b. Presentation to ERIC of data collection materials and approach
    c. Documentation of assessment approach as agreed upon by both parties
    d. Matrix listing all needed data elements
2. Project execution
    a. Weekly status reports from the selected BIDDER to ERIC staff
3. Policy and procedure assessment report including:
    a. Statement of ISO alignment
    b. Statement of compliance by ERIC staff to existing ERIC policies and procedures
    c. Recommendations for improvements, including additional alignment to ISO or other standards
4. Specific test results
    a. Vulnerability scan report of possible vulnerabilities and what steps are necessary to mitigate them.
    b. Penetration testing report describing methods used to attempt to gain access, results of attempts, and what steps are necessary to mitigate them.

c. Social engineering test report describing methods used, results of attempts, and suggestions for improvements.
d. Email configuration assessment report of possible vulnerabilities and what steps are necessary to mitigate them.
e. Hashing application code review report

5. Final Report (internal, confidential)
   a. Summary of work performed
   b. Findings of significant threats or vulnerabilities to ERIC and recommendations to mitigate any findings
   c. Recommendations for additional areas of assessment that were not included in this project
6. Executive Summary that can be shared with stakeholders (public, non-confidential)

Work Approach

The ERIC infrastructure involves four offices and a vendor-managed data center. Due to the distributed nature of ERIC operations:

1. It is anticipated that a majority of the work will be performed at the selected BIDDER's premises.
2. Selected BIDDER will submit a weekly status report to ERIC staff. The selected BIDDER and ERIC staff will establish the general content of the weekly status reports.
3. ERIC and data center vendor management and staff will be available for phone or web conference interviews.
4. If in-person interviews of ERIC staff members are necessary, the ERIC staff will travel to Portland, Oregon, bringing ERIC laptops.
5. No onsite visit of the ERIC data center or ERIC staff offices is intended in this assessment.
6. Remote access to ERIC staff offices will be accommodated, as necessary.
7. Some cloud services are used for shared resources, outside and not connected to the ERIC data center, and ERIC's use of these services should be included in the assessment.

Procurement Schedule

Milestone	Estimated Date
Release RFP to BIDDERS	April 8, 2019
BIDDER questions (if any) and letter of intent due	April 22, 2019
Answers to RFP questions released	April 26, 2019
Proposal responses due	May 20, 2019
Finalists selected (on or before)	May 28, 2019
BIDDER interviews if needed (please reserve these dates)	June 3-5, 2019
BIDDER Selection	June 13, 2019

Letter of Intent

Firms planning to submit proposals are strongly encouraged to provide a written letter of intent to propose by April 22, 2019. An email attachment sent to shane.hamlin@ericstates.org is acceptable. The letter must identify the name, address, phone, and email address of the person who will serve as the key contact for all correspondence regarding this RFP.

A letter of intent is required in order for ERIC to provide interested BIDDERs with a list of any questions received and ERIC's answers to those questions. Those providing a letter of intent will also be notified of any addenda that are issued.

BIDDERS who choose not to provide a letter of intent will be responsible for monitoring ERIC's website for any addenda issued for this RFP.

PROPOSAL REQUIREMENTS

The proposal must include the following:

1. A summary of the proposal and the BIDDING firm's qualifications to perform the scope of work and successfully complete the deliverables identified in this RFP. The summary may also articulate why the firm is pursuing this work and how it is uniquely qualified to perform it.
2. Affirmation of the BIDDING firm's willingness to agree to/adhere to a Non-Disclosure Agreement concerning the protection of confidential information shared or reviewed during the assessment, pursuant to ERIC's information security policies.
3. Basic information about the BIDDING firm, including:
    a. Company name, name and title of contact person, company address, phone, email address and company website.
    b. Description of its corporate footprint; describe whether the firm is local, regional, national or international.
    c. Brief description of the firm and the characteristics that set it apart.
    d. Year the firm was founded, whether it is a private or public company, and the extent to which there is any foreign ownership/investment in the company.
4. Brief description of the BIDDING firm's practices, guidelines or certifications for protecting and handling secure and private information about and for its clients.
5. Scope of Services
    a. A detailed plan of how the firm will approach the security assessment, meet the project objectives, and achieve the deliverables identified in this RFP.
6. Price Proposal
    a. The price proposal must include the following statement: "Proposal and cost schedule shall be valid and binding for ONE HUNDRED EIGHTY (180) days following proposal due date and will become part of the contract that is negotiated with ERIC."
7. Clear statement on whether the BIDDING firm plans to subcontract or partner with another firm for the assessment
    a. If subcontracting or partnering with another firm, identify the work that will be performed by the subcontractor/partner firm.
    b. For subcontractor/partnering firm staff, provide all the information listed below for key project staff background information
8. Key project staff background information
    a. Staff member name
    b. Position in the company
    c. Length of time in this position
    d. Length of time with the firm
    e. Project position and responsibilities
    f. Education
    g. Previous work experience
    h. Skills and qualifications, including any relevant certifications

i. Evidence of criminal background check completed in the preceding 24 months. If a background check has not been completed in the preceding 24 months, affirm willingness to complete a criminal background check prior to project kick-off.

9. Customer References, including:
    a. Customer/client name
    b. Reference's name
    c. Title
    d. Phone number
    e. Email
    f. Project description
    g. Start and end date for the project
    h. Contract amount
10. At least two example reports from previous similar work. Any information submitted as part of the proposal is presumed not confidential. However, sensitive customer information may be redacted if necessary.
11. A copy of your firm's current terms and conditions.
12. A person who is legally authorized to bind BIDDER to a contract with ERIC must sign the proposal.

Evaluation Process

ERIC staff, members of ERIC's Board of Directors or their designees, and members of ERIC's Privacy and Technology Advisory Board may evaluate the submitted proposals.

The evaluators will consider how well the BIDDER's proposed methodology and deliverables meet the needs of ERIC as described in the BIDDER's response to each requirement. It is important that the responses be clear and complete so that the evaluators can adequately understand all aspects of the proposal. The evaluation process is not designed to simply award the contract to the lowest cost BIDDER. Rather, it is intended to help ERIC select the BIDDER with the best combination of attributes, including price, based on the evaluation factors.

ERIC may ask BIDDERS to make a presentation to a selection team, although ERIC reserves the right to award without presentations. Presentations will be made via webinar and conference call.

Other Considerations

The sole point of contact for questions and additional information concerning this RFP is Shane Hamlin, Executive Director of ERIC.

Phone: (360) 789-0786
Email: shane.hamlin@ericstates.org

The Information Security Assessment Project Manager is Ericka Haas, ERIC Systems Engineer and Technical Liaison. Once a BIDDER is selected, Ericka will be the primary point of contact for the Information Security Assessment project.

While additional information presented in response to BIDDER questions will be helpful in clarifying ERIC's expectations pursuant to the RFP, only this RFP and any subsequent written amendments or statements issued by the Executive Director will be definitive regarding ERIC's RFP requirements for the resulting security assessment.

This RFP is not an offer to contract and commits ERIC to no further actions. ERIC shall not be obligated in any manner to any BIDDER until a written agreement has been executed between ERIC and the selected BIDDER relating to the approved bid.

ERIC is not responsible for any BIDDER's direct or indirect costs to prepare a response to this RFP.

The selected BIDDER must be able to commit to providing resources for the completion of the assessment and all deliverables by the agreed-upon completion date. ERIC would prefer to reach an agreed-upon completion date that is prior to December 1, 2019.

ERIC will own all rights, including the copyright, of all the deliverables produced as a result of the Information Security Assessment.