State of North Carolina
Department of the Secretary of State

ELAINE F. MARSHALL
SECRETARY OF STATE

ANN B. WALL
GENERAL COUNSEL

AGENCY: N.C. Department of the Secretary of State, Notary Enforcement Division.

ACTION: Advance Notice of Proposed Rulemaking (ANPR #2) and Request for Public Comments

DEADLINE FOR SUBMITTING COMMENTS: 11:59 p.m. on May 15, 2023

ADVANCE NOTICE OF PROPOSED RULEMAKING AND REQUEST FOR PUBLIC COMMENTS (ANPR #2)

The Department of the Secretary of State is issuing this advance notice of proposed rulemaking (ANPR #2) to request public comment on significant questions related to the technical features, components, specifications and standards required for the implementation of the Remote Electronic Notarization Act (RENA) which became effective July 8, 2022. N.C. Session Law 2022-54. RENA primarily amends Article 2 of Chapter 10B, Notary Public Act, in the North Carolina General Statutes, and those changes have been codified at G.S. 10B-134 *et seq.* Adoption of RENA was a direct outcome of the global pandemic, which increased the "remote" conduct of economic activity and established the necessity to conduct crucial business, legal, healthcare, and other transactions safely, securely and efficiently in the rapidly changing remote environment.

There is visible, widespread interest in the implementation of RENA. The Secretary is publishing this ANPR in order to provide stakeholders with an early opportunity to provide input into the rules that the Secretary must draft in order to implement RENA.

RENA directs the Secretary to adopt permanent rules on a large number of topics. In promulgating those rules, the Secretary must comply with the N.C. Administrative Procedure Act.[1] The goal is to establish procedures that will promote public confidence in the reliability of signatures and the identification of remotely located principals to ensure that transactions are not repudiated as a result of:

1. Mental incapacity of the principal;
2. Coercion or duress; or
3. Fraud.

By enhancing reliability, the Secretary facilitates economic growth while reducing costly and avoidable litigation.

[1] G.S. 150B-1, 150B-2(8a)d.

HOW THIS ANPR DIFFERS FROM THE FIRST: The Secretary previously published an Advance Notice of Proposed Rulemaking and Request for Public Comments on October 11, 2022 (ANPR #1). In ANPR #1, the Secretary sought input on the role of the remote electronic notary public (RENP) and the general procedures and standards needed to implement RENA to ensure the effectiveness, efficiency and integrity of the notarial acts and processes contemplated under RENA. The period within which to submit comments to ANPR #1 is closed.

In this ANPR #2 the Secretary seeks public input on the technical features, components, specifications and standards required by RENA and applicable to the communication, credential analysis, and identity proofing described in the statute. The Secretary also seeks public input on the processes applicable to licensing platforms and approving third-party vendors. Although the Secretary is not required to request public comment at this stage of the rulemaking process, the Secretary nonetheless requests stakeholder input to provide for a well-informed, transparent rulemaking process that leads to effective, comprehensive, and understandable permanent rules.

RENA allows qualified Notaries Public and certain principals to complete a remote electronic notarial act even if the notary and the principal are in different physical locations. These parties must use real time online communication technology authorized by the Secretary and the performance of the remote electronic notarial act (REN) may take place only after proper identification of the principal. At the time of the REN, the notary (which in most instances must be an electronic notary) must be physically located in North Carolina, while the principal may be located anywhere inside the United States or, under certain circumstances, at U.S. military installations or U.S. embassies.

All notaries who perform remote online notarizations will be required to use platforms licensed by the Secretary, as well as credential analysis and identity proofing technologies approved by the Secretary. Rulemaking is required to clarify the overall process, to protect notaries, principals, and the public against fraud, and to supply licensed platforms and approved third-party vendors with the specificity necessary to provide technology solutions that perform as required by statute.

Technology threats and vulnerabilities are constantly evolving, while laws and regulations often take years to develop and even longer to amend. It is a near certainty that whatever security standards represent best practices today may no longer be adequate in five years' time. Therefore, it is a goal of this rulemaking to adopt rules that establish reasonable administrative, technical, and physical data practices and procedures to protect and secure covered transactions and resulting data from unauthorized access, modification, and acquisition, and that also have sufficient flexibility to require technology improvements as threats and vulnerabilities evolve over time.

TRADE SECRETS: Some responses to these questions may include confidential or trade secret information. To protect such confidentiality, the responder must comply with the specific requirements of North Carolina law: the N.C. Public Records Act, G.S. 132-1.2, and G.S. Chapter 66, Article 24, Trade Secrets Protection Act.

ABOUT THE RULEMAKING PROCESS: The Secretary is not required to request public comment at this stage of the rulemaking process. The public will also have the opportunity to comment upon the proposed rules once they are published in the North Carolina Register. North Carolina law requires that the public have at least 60 days to comment upon proposed rules. During the public comment period, the Secretary anticipates conducting at least one public hearing to receive comments. After the public comment period closes, the Secretary will review the comments received and as a result may make changes to the rules. The Secretary then formally adopts the rules, which subsequently must be submitted to the N.C. Rules Review Commission (RRC). RRC is a legislatively appointed commission which may request changes to the content of the rules. RRC may also object to any of the rules on the grounds that they are: ambiguous, outside statutory authority, not reasonably necessary, or that proper procedures were not followed. Depending on the comments or objections from RRC, the Secretary may make changes to the rules and re-submit them to RRC. There are additional steps in the rulemaking process not described here.

If you are interested in receiving notices related to the RENA rulemaking process, please subscribe to the Secretary's rulemaking interested persons list. Instructions for subscribing may be found at https://sosnc.gov/divisions/general_counsel/rulemaking_interested_person_mailing_list or by following the link at www.sosnc.gov/rulemaking.

HOW TO SUBMIT COMMENTS: In order to submit comments, you must:

1. Put 'RENA ANPR #2' in the subject line of any submittal cover page or cover email,
2. Include your name and contact information,
3. If you are commenting on behalf of a business or organization, please indicate which one, and
4. Include the question number to which your comments respond.

ADDRESS COMMENTS TO: Ann. B. Wall, General Counsel and Rulemaking Coordinator, N.C. Department of the Secretary of State. Note that all comments are subject to the public records provisions of G.S. 132-1, *et seq.*

SUBMIT COMMENTS BY:

1. Emailing comments to ANPR@sosnc.gov,
2. USPS to: P.O. Box 29622, Raleigh, NC 27626-0622, or
3. Courier service (ex. UPS, Fed Ex) to: 2 South Salisbury Street, Raleigh, NC 27601.

FOR FURTHER INFORMATION: Email the Secretary at ANPR@sosnc.gov or visit www.sosnc.gov/rulemaking.

Contents

Glossary

Glossary Term	Definition
ANPR	The Advance Notice of Proposed Rulemaking.
CISO	Chief Information Security Officer or its equivalent.
CT Recording	The communication technology recording defined in RENA as "the simultaneous, synchronous audio and visual recording of the notarial act."[2]
Electronic notary	Notary Public registered with the Secretary in conformance with Article 2 of Chapter 10B of the N.C. General Statutes with the authority to perform electronic notarial acts.
Identity verification technology	Technology that performs either credential analysis, identity proofing, or both.
Information security, information security standards, IT security	For purposes of this ANPR #2, these phrases include confidentiality and privacy, availability, security, and integrity of both data and technology.[3]
ISO	International Standards Organization.
IT	Information Technology.
NIST	National Institute of Standards and Technology.
PII	Personally Identifiable Information.
REN	Remote Electronic Notarization as defined in RENA.[4]
RENA	The Remote Electronic Notarization Act, House Bill 776, Session Law 2022-54, as well as any RENA-related rules adopted by the Secretary.
RENA-Qualified	For purposes of this ANPR #2, this phrase includes both the requirements of the RENA statute and of any rules that the Secretary may adopt.
RENP, remote electronic notary	The Remote Electronic Notary Public as currently defined in RENA.[5]
RLP	Remotely Located Principal as defined in RENA.[6]
Secretary	The North Carolina Secretary of State.

[2] G.S. 10B-134.1(1).
[3] 44 U.S.C. 3542 (b)(1) provides:
> The term ''information security'' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
> (C) availability, which means ensuring timely and reliable access to and use of information.

[4] G.S. 10B-134.1(8).
[5] G.S. 10B-134.1(9).
[6] G.S. 10B-134.1(10).

Third-party vendor	For purposes of this ANPR #2, unless otherwise indicated, this phrase includes third-party vendors performing credential analysis, identity proofing, and custodial services such as depositories and stewards.

A. Application, Renewal, and Reinstatement – Definitional issues.

RENA directs the Secretary to adopt rules to establish standards, procedures and practices regarding the security, features and other matters related to communication technology, credential analysis and identity proofing.[7] RENA also establishes criteria under which the Secretary will evaluate a platform license application.[8] RENA defines a "platform" [9] as the online system that utilizes communication technology to perform the remote electronic notarial act (REN). RENA separately defines "communication technology" as:

> An electronic device, process, or system that allows a remote electronic notary and a remotely located principal to communicate with each other simultaneously by sight and sound using audiovisual technology and that makes reasonable accommodations for remotely located principals with vision, hearing, or speech impairments.[10]

The Secretary must issue platform licenses to prospective platform providers after reviewing the functionality, operational standards and security of the technology and determining that they are RENA-qualified.[11] The Secretary shall determine the manner of annual platform license renewals.[12]

RENA also requires that the Secretary approve "third-party vendors."[13] RENA defines "third-party vendor" as "[a] person providing credential analysis, identity proofing, or custodial services to remote electronic notaries."[14] RENA provides definitions for "credential analysis"[15] and "identity proofing,"[16] but not for "custodial services." Custodial services" are likely to include "secure storage of the electronic journal,"[17] "acting as a depository electronic journal,"[18] "retention of the journal for 10 years,"[19] and serving as a "steward," [20] a term not defined within the statute.

These third-party vendors provide components essential to platform functionality. Whether approval of the third-party vendors providing these essential components will be subject to the platform licensure process has not yet been determined. The Secretary requests comments on the following questions:

Question A.1. Are there actual market conditions under which third-party vendors will not provide their services in connection with a platform?

Question A.1.a. If third-party vendors do not provide services in connection with a platform, should the Secretary nonetheless establish performance and security standards for these third-party vendor services since they are integral to performing remote electronic notarization duties successfully?

Question A.1.b. Is there a statutory basis for the Secretary to license or otherwise establish performance and security standards for third-party technologies that stand alone from and are not incorporated into a platform? Please provide a detailed analysis in support of your position.

---

[7] G.S. 10B-134.21.
[8] G.S. 10B-134.19.
[9] G.S. 10B-134.1(6).
[10] G.S. 10B-134.1(1).
[11] G.S. 10B-134.19(b).
[12] G.S. 10B-134.19(f).
[13] G.S. 10B-134.11(a)(2)a-b, 10B-134.15(b)(4), 10B-134.17(a)(1), 10B-134.23.
[14] G.S. 10B-134.1(12).
[15] G.S. 10B-134.1(3).
[16] G.S. 10B-134.1(5).
[17] G.S. 10B-134.15(b).
[18] G.S. 10B-134.15(b)(4).
[19] G.S. 10B-134.15(b)(2).
[20] G.S. 10B-134.17(a)(1).

Question A.2. Will it aid RENPs, third-party vendors or any other members of the public if the Secretary defines "custodial services"? If "yes," should the definition limit the allowed custodial services to:

- Secure storage of the electronic journal,
- Acting as a depository electronic journal,
- Retention of the journal for 10 years, and
- Serving as a steward?

Or should other services be included? If other services should be included, please explain.

The Secretary shall review and issue platform licenses to "qualified applicants."[21] Platform licenses shall be renewed annually "in a manner set by the Secretary."[22] RENA directs the Secretary to "adopt rules as necessary to establish standards, procedures, practices, forms, and records" relating to "the security standards, features, qualifications, measures, storage and any other matter related to communication technology, credential analysis and identity proofing."[23]

Question A.3 Is there any compelling reason why the Secretary should *not* review for compliance with applicable standards:

- Third-party vendor technologies?
- Renewal applications of platforms or third-party vendor technologies?

Please explain and provide statutory citations where appropriate.

Platforms and third-party vendors will necessarily have access to, and may hold for an extended time, information that may be personal or confidential. The information may be about remote electronic notaries public (RENPs), remotely located principals (RLPs), transactions, and parties to transactions. Personally identifying information (PII) may be present on documents used to verify the identity of the RLP. The premature disclosure of a significant commercial transaction involving a remote electronic notarization has the potential to move markets. The electronic journal must be retained in an approved secure storage for at least ten years.[24] There is the possibility that the CT Recording must be retained for a substantial period of time as well. *See generally* discussion in ANPR #1.

The Secretary must issue platform licenses to RENA-qualified applicants.[25] The application must describe the technology proposed to address identity verification and geolocation requirements. It must include explanations regarding IT security governance and the designation of a chief information security officer (CISO) or equivalent.[26] The application is to include the names of all officers or directors directly involved in the operation, management or control of the platform, and all employees who exercise substantial influence or control over the platform. RENA requires the Secretary to conduct background investigations of all persons named in the application, as the Secretary deems necessary.[27] The background investigation shall include a criminal history check of the applicant and persons described in the application.[28] The Secretary must determine that the applicant is of good moral character, and that the communication technology meets the performance and security requirements of RENA.[29] The Secretary's review may include other elements.[30] For example, the review elements might include demonstrating the economic stability of the applicant or other economic assurances in order to ensure safe, secure, and accessible storage of the electronic journal and CT Recordings over time.

[21] G.S. 10B-134.19(b).
[22] G.S. 10B-134.19(f).
[23] G.S. 10B-134.21(a)(3).
[24] G.S. 10B-134.15(b)(2).
[25] G.S. 10B-134.19(b).
[26] G.S. 10B-134.19(c)(3).
[27] G.S. 10B-134.19(d).
[28] *Id*.
[29] G.S. 10B-134.19(e).
[30] G.S. 10B-134.19, 10B-134.21.

A.4. Officers and Directors

RENA mandates that a completed application include "the names of all officers or directors directly involved in the operation, management, or control of the platform."[31] The Secretary must conduct background investigations as necessary, including criminal history record checks, for each of the listed officers and directors.[32] RENA does not include definitions of "operation . . . of the platform," "management . . . of the platform," or "control of the platform." The applicants, the individuals to be named, and the Secretary will benefit if these terms are defined. The Secretary is aware that there are both State and federal permitting and licensure laws with similar requirements. The Secretary invites stakeholders to comment on the following questions:

Question A.4.a. Are there North Carolina or federal definitions for any of the following RENA terms that the Secretary should consider in drafting the rules? If yes, please provide the statutory citation to suggested definitions and the reason you think it appropriate for use in RENA rules. The terms are:

- Directly involved
- Operation . . . of the platform
- Management . . . of the platform
- Control of the platform
- Officer or Director "directly involved in the operation . . . of the platform"
- Officer or Director "directly involved in the management . . . of the platform"
- Officer or Director "directly involved in the control of the platform."

Question A.4.b. Is there an industry standard definition or other definition for the terms listed in question A.4.a that the Secretary should consider? If yes, please provide a citation and location where the standard can be found, or provide a copy of the standard.

Question A.4.c. If the licensure of a platform will include approval of components provided by third-party vendors, should the requirements applying to officers and directors of the platform also apply to the third-party vendors, or would certification from platforms that they have performed appropriate vendor analysis be sufficient? Please explain your answer.

A.5. Employees

RENA requires that the platform application include the names of "all employees who exercise substantial influence or control over the platform."[33] The Secretary must also conduct background investigations, including criminal history record checks, for the named employees.[34] RENA does not include definitions of "employees," "influence," "substantial influence," "control" or "substantial control."

The Secretary is aware of the IT industry's vitality, energy, creativity, entrepreneurial, and ever-changing nature. The industry has high employee turnover rates. Use of contractors in software development is ubiquitous. The danger of rogue insiders can lead to significant IT security compromises and cyber events. Regardless of their employment status, those who write the computer code and programs and maintain the REN-related IT systems will have significant impact on the IT security, and effectiveness of platform and third-party vendor technology.

A definition of "employee" who exercises substantial influence or control over the platform in the RENA rules must be understandable to all parties. The Secretary requests comment on the following questions related to the definition of "employee." Please provide a detailed explanation of your response, including citations to law, rule, regulation, or standards as appropriate. The questions are:

[31] G.S. 10B-134.19(c)(2).
[32] G.S. 10B-134.19(d).
[33] G.S. 10B-134.19(c)(2).
[34] G.S. 10B-134.19(d).

Question A.5.a. Are there state or federal law or industry or other standards for terms listed below that might be applicable in the RENA context? If yes, please provide the sources and the reason you think it appropriate for use in RENA rules. The terms are:

- Employee
- Influence
- Control
- Substantial influence
- Substantial control
- Exercise substantial influence
- Exercise substantial control

Question A.5.b. Should the definition of "employee" be limited to a person whom the applicant employs directly, or in this context does it also include a contractor?

Question A.5.c. When defining the phrase "exercising substantial influence or control over [a] platform":

Question A.5.c.1. Are there words or phrases unique to the industry and well-understood by it and others that the Secretary should consider using to make the definition more understandable?

Question A.5.c.2. Are there words or phrases that the Secretary should avoid including in the definition?

Question A.5.d. Are there any other factors or elements that the Secretary should consider when defining "employees who exercise substantial influence or control over the platform"? If yes, please explain and be specific.

B. Application, Renewal, and Reinstatement - Background Investigations

The Secretary is required to "review and issue platform licenses to qualified applicants."[35] The Secretary will review the application, conduct background investigations "as deemed necessary,"[36] and determine whether the applicant can meet all RENA functionality requirements, including:

- Identify proofing
- Credential analysis
- Security
- Confidentiality
- Secure storage
- Geolocation.[37]

Background investigations will cover not only the platform applicant but also all named officers, directors, and employees.[38] Background investigations must include criminal history record checks, to which the individuals must consent.[39] RENA does not define "background investigations." The apparent purpose of the background investigations is not only to verify application information but to help determine if the platform applicant is "of good moral character." RENA does not define "good moral character." Background investigations may provide insight regarding security and integrity of the platform and its components and if it is likely to be intentionally compromised. All of these bear on whether the Secretary should grant a license to the applicant.[40]

B.1. Background investigation of the platform applicant itself.

The Secretary is aware that platforms will belong to a volatile and quickly-evolving IT sector. The economic stability of the platform applicants' businesses will impact their capacity to fulfill the requirements of RENA, including IT security (confidentiality, integrity and availability) and records retention. The Secretary expects that industry stakeholders may have suggestions as to how best to evaluate, for example, the economic stability of a

[35] G.S. 10B-134.19(b).
[36] G.S. 10B-134.19(d).
[37] G.S. 10B-134.19(e).
[38] G.S. 10B-134.19(d).
[39] *Id.*
[40] G.S. 10B-134.19(e).

platform applicant. Please provide detailed responses, with citations to pertinent laws, rules or regulations, and industry or other standards.

What questions about the applicant's history will most effectively provide the Secretary with information necessary to evaluate the application? For example, should the application:

Question B.1.a. Be limited to information likely to reveal a history of fraud or deceptive practices, such as criminal history, license status or disciplinary actions before other state or federal agencies, debarment, and the like?

Question B.1.b. Information about intellectual property infringement notices received, judgments against or the financial strength of the applicant?

Question B.1.c. Other? If yes, what? Be specific.

B.2. Background investigation of the platform applicant's officers and directors directly involved in the operation, management, or control of the platform.

The platform applicant must name its designated Chief Information Security Officer (CISO) or equivalent in the application. The equivalent will be any individual functioning in the capacity of, and performing the duties of, CISO regardless of title.

Question B.2. Are there any officers or directors other than the designated CISO or equivalent who should be presumed to be "directly involved in the operation, management, or control of the platform"?

Question B.2.a. If yes, to which officers and directors should the presumption apply? Would these additional officers include or be limited to Chief Information Officer, Chief Privacy Officer, and Chief Technology Officer, and why? Please be specific.

Question B.2.b. If no, why not?

B.3. Background investigation of the platform applicant's employees who exercise substantial influence or control over the platform.

Question B.3. Are there specific categories of employees that should be presumed to exercise substantial influence or control over the platform? Please be specific.

B.4. Background Investigation – general questions.

RENA provides little guidance as to how the Secretary is to evaluate the "good moral character" of the platform applicants. The Secretary would appreciate comment from the stakeholders and other respondents to this ANPR #2 with regard to how the investigation results should be considered in making a decision.

Question B.4.a. Are there industry standards or peer-reviewed studies of the elements of character that have enabled IT sector businesses to successfully, effectively, securely, confidentially, and lawfully provide services? If yes, please provide the information necessary for the Secretary to review the studies.

Question B.4.b. Is there case law in which the courts have found that the character of an IT sector business contributed to its failure to successfully, effectively, and lawfully provide services, including confidentiality and security of information?

Question B.4.c. If stakeholders and other respondents are aware of moral character factors or standards that the Secretary should consider in determining whether a platform applicant should be licensed, please list them, and explain.

Question B.4.c.1. For example, is there any reason why the Secretary should *not* consider an applicant's federal security clearance or denial of clearance as relevant to a determination of good moral character?

Certain financial conditions can increase susceptibility to bribery, blackmail, and temptations to modify processes, procedures, and siphon off funds and access and use confidential information inappropriately.

Question B.4.d. Should the Secretary's background investigations explore the financial condition of named officers, directors, and employees?

Question B.4.d.1. If no, why not? Please provide a detailed explanation, with any legal basis for the position taken.

Question B.4.e. Are there other factors (such as employment history) that the Secretary should evaluate for named officers, directors, and employees when considering the moral character of platform applicants?

B.5. Application, Renewal, and Reinstatement – Renewal Applications and Reinstatements

Platform licenses must be "renewed annually in a manner set by the Secretary."[41] RENA is silent whether third-party vendor approvals must be renewed annually.

Question B.5.a Is there any reason why third-party vendor information should *not* be included with the annual license renewals of platforms?

Question B.5.b. Is there any reason why the Secretary should not review each renewal application with the same level of scrutiny as an initial application?

Question B.5.c. What changes to the initial application may be considered of such a non-substantive nature that they may be deemed "ministerial" and not meriting further review during the renewal application process?

Question B.5.d. Should the applicant be required to notify the Secretary of material changes to information supplied in an application or renewal before the next renewal application is due (*i.e.,* a material change might include a change in the individuals named, a security compromise, a material deterioration in financial condition, a debarment, or the filing of a criminal action against the applicant or any of the individuals named)?

Question B.5.d.1. Should notice of such material change of information trigger immediate review of the existing license by the Secretary?

C. Audio-Video Communication

RENA includes a number of requirements regarding the effectiveness of the communication between the RENP and the RLP. The requirements include that the communication be:

- Simultaneous, by sight and sound, with accommodations for RLPs with vision, hearing, or speech impairments;[42]
- Real-time;[43]
- Have audio with sound clear enough that each participant can "hear and understand all other participants;"[44]
- "Have sufficient video quality to allow a clear and unobstructed visual observation of the face of each participant and any identification provided by the remotely located principal for a sufficient time to allow the remote electronic notary to verify the remotely located principal's identity."[45]

The purpose of these requirements is to assure the integrity of the notarial process by reducing opportunities to exploit the remote technology in the pursuit of fraud.

C.1. Audio communications.

"Real-time" and "simultaneous" are not defined in RENA. Due to technology constraints, "real-time" and "simultaneous" communication always involves a delay between the time when one person speaks and the other responds. Such delays can become noticeable to even the most casual observer, particularly where connections are

[41] G.S. 10B-134.19(f).
[42] G.S. 10B-134.1(1), 10B-134.5(2).
[43] G.S. 10B-134.5(a)(1).
[44] G.S. 10B-134.5(a)(3).
[45] G.S. 10B-134.5(a)(4).

poor or communication traffic is heavy.

The Secretary is not aware of state or federal regulations that define "real-time" and "simultaneous," or that address readily apparent audio-visual lag time between one person asking a question and the other responding. Similarly, the Secretary is not aware of industry or other standards in this regard.

The Secretary requests input from stakeholders regarding how the rules might be written to ensure that:

- All of the RENA communication requirements are fulfilled.
- Allowance is made for IT advances, with limited need for additional rulemaking.
- The RENP, the Secretary, and those directly dependent on the reliability of the REN can determine if the real-time and simultaneity requirements are satisfied during a particular session.

For each of the following questions, the Secretary requests that respondents provide detail and citations to law, rules and regulations, and industry or other standards.

Question C.1.a. Which state or federal laws, rules or regulations or industry or other standards define "real-time" and "simultaneous" in a way that may be helpful to the Secretary in drafting rules? Please provide citations for them. If a particular definition is deemed preferable, please note that and explain why.

Question C.1.b. Is there an objective measure of lag times that pose an unacceptable security vulnerability subject to exploitation? Should a determination that there is an unacceptable time lag rest upon the subjective judgment of an RENP? How would the RENP determine such an unacceptable time lag is occurring?

Question C.1.c. Is there an acceptable amount of asynchronicity between the spoken words and the movement of the speaker's mouth that does *not* pose an unacceptable security vulnerability subject to exploitation? How would the RENP determine such an acceptable amount of asynchronicity is occurring?

Remote communications between individuals can become difficult to understand at times. These communications can become blurry or include audio interference. Remote communications can break up, be scratchy, muddy, harsh, or sibilant. They can otherwise be uncomfortable or somewhat unintelligible. Any of these issues would signify that the audio or visual component of the communication is not clear enough to be understood and used in the REN. It might be helpful to the regulated community if the rules use terminology specific to the communication industry.

Question C.1.d. Are there words or phrases defined in state or federal law, rule, or regulation, or minimum industry standards or technical specifications that specifically describe the technical qualities of an audio-visual communication to ensure that it has:

- Sound clear enough to be understood,
- Video of a quality sufficient to permit observation of the RLP and any identification presented and
- No unacceptable security risk.

C.2. Video communications.

The only guidance that RENA provides regarding video communication is that it must be of "sufficient" quality "to allow a clear and unobstructed visual observation of the face of each participant and any identification provided by the remotely located principal to allow the [RENP] to verify the [RLP's] identity."[46] RENA does not define:

1. "sufficient quality,"
2. "clear," or
3. "unobstructed visual observation."

Question C.2.a. Should the three terms above be defined to provide clarity to technology vendors and the RENP?

Question C.2.a.1. If so, are there laws, rules, regulations, industry, or other technical standards the Secretary should evaluate in preparing such definitions? Please provide the citations for any such definitions.

[46] G.S. 134-5(a)(4).

Question C.2.a.2. If there is a preferred definition, please note that fact and explain why it is preferred.

The quality of the video communication is integral to identification of the RLP by the RENP. Quality audio-video communication also allows the RENP to make the observations necessary for a determination that the RLP is not "in the judgment of the notary incompetent, lacking in understanding of the nature and consequences of the transaction requiring the notarial act, or acting involuntarily, under duress, or undue influence."[47]

Video clarity may be a function of the capacity of:

- The camera sending the video, including picture pixel capacity and positioning.
- The screen displaying the video, including pixel picture receipt and display capacity.
- Transmission speed.
- Internet connection speed.
- Lighting and coloring of the sender's and recipient's environment.
- Filters or other factors.

Question C.2.b. If there are other video quality-related factors that the Secretary should take into account when drafting rules related to accommodation of persons with visual, speech or hearing impairments, what are they? Please be specific.

D. Identity Verification Technology– Identity Proofing and Credential Analysis

Verification of the identity of the principal in a notarial act is fundamental to prevention of fraud and ensuring the smooth flow of economic and other transactions. Traditional and electronic notaries public conducting an in-person notarial act may verify the principal's identity by any of three means: (1) The notary's personal knowledge of the principal's identity, (2) a credible witness, or (3) satisfactory evidence of the principal's identity.[48] "Personal knowledge," "credible witness," and "satisfactory evidence" are defined terms.[49] Regardless of the type of notary public, the notary shall not perform a notarial act if the identity of the principal cannot be verified.[50]

Unlike identity verification at a traditional in-person notarial event, RENA specifically describes two methods for identity verification of the RLP:[51]

(1) The RENP's personal knowledge of the RLP's identity,[52] or

(2)(a) Credential analysis by an approved third-party vendor plus (b) identity proofing by an approved third-party vendor plus (c) RENP comparison of the RLP's identification document with the RLP's face on screen.[53]

Identity verification should not be confused with identity authentication. Identity verification requires the positive identification of a person who more often than not does not have a previous relationship with the RENP. Identity authentication, on the other hand, is the process of authenticating that a person is the same person who has been at a site previously. Identity authentication typically involves passwords, multi-factor authentication, physical tokens, or other similar processes. Identity authentication has no direct relevance to the identity verification that RENA tasks the RENP with undertaking.

RENA defines "identity proofing" as a "process or service through which a third-party vendor affirms the identity of a remotely located principal through review of personal information from public or proprietary data sources."[54] Neither "public or proprietary data sources" nor "personal information" are defined terms in RENA.

---

[47] G.S. 10B-40(a2)(2).
[48] G.S. 10B-3(1), (2), (14).
[49] G.S. 10B-3.
[50] G.S. 10B-20(c)(2), (2a); 10B-116(2); 134.3(b)(1).
[51] However, as noted in the Agency's first ANPR, it is not clear whether a "credible witness" can be used to prove the identity of the RLP under RENA because, through there is no direct prohibition against such use in RENA, there is no specific authorization for such use, either. G.S. 10B-102(a)("Article 1 of this Chapter applies to all acts authorized under this Article unless the provisions of Article 1 directly conflict with the provisions of this Article").
[52] G.S. 10B-134.11(a)(1).
[53] G.S. 10B-134.11(a)(2).
[54] G.S. 10B-134.1(5).

"Credential analysis" is a "process or service through which a third-party vendor performs a remote analysis of the characteristics and security features of each identification credential presented by the remotely located principal pursuant to G.S. 10B-3(22)a."[55] G.S. 10B-3(22)a. requires a principal to present "at least one current document issued by a federal, state, or federal or state-recognized tribal government agency bearing the photographic image of the individual's face and either the signature or a physical description of the individual." There is no definition of the "characteristics and security features" to be analyzed in the identification document presented for credential analysis.

RENA does not say whether the identify verification technologies must be accurate 100% of the time, or if there is some rate of false acceptance and false denial that will nonetheless be acceptable and meet the reliability standards expected in the context of notarial identification. There are reports that identity-proofing processes such as knowledge-based authentication (KBA) may have false rejection rates of as much as 25%.[56] A study by a vendor and a national contact center showed that "at one institution fraudsters passed KBAs 92% of the time, while genuine customers only passed KBA's 46% of the time."[57] Organized crime rings reportedly have set up storefronts on the dark web and have become illicit data vendors of personal information--even offering return policies.[58] Moreover, "[t]he risk that an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and impersonate that individual led the National Institute of Standards and Technology (NIST) to issue guidance in 2017 that effectively prohibits agencies from using knowledge based verification for sensitive applications"[59] and prompted the Government Accounting Office to recommend that named federal agencies "develop a plan with time frames and milestones to discontinue knowledge-based verification."[60]As much as 12% of the time, retail and insurance company agents failed to verify customers' identities.[61]

The Secretary must adopt rules for security standards, features, qualifications, measures, storage, and any other matter related to identity verification technologies,[62] as well as rules that require maintaining the confidentiality of both the questions asked as part of any identity proofing and the means and methods of the credential analysis.[63]

If the third-party vendor's identity verification technology does not indicate a match to the identity offered by the RLP, absent any rule to the contrary the third-party vendor might elect to permit the RLP to go through the identity verification procedures a second or even third time. At some point when the identity verification process has failed to positively identify the RLP, the vendor must inform the RENP of that fact.

If public or proprietary sources used to identity proof include incorrect personal information, then that, too, could lead to false rejection of an RLP as not identity-proofed. For example, if identity proofing were to include asking the RLP questions based on incorrect information from a proprietary source, the RLP would necessarily answer incorrectly, potentially leading to rejection of the RLP's identity proof. Similarly, there are widespread reports of

---

[55] G.S. 10B-134.1(3).
[56] *E.g., "Free": The True Costs of Knowledge Based Authentication Questions?* Pindrop Blog (Oct. 12, 2021), https://www.pindrop.com/blog/the-true-costs-of-knowledge-based-authentication-questions#:~:text=According%20to%20a%20Forrester%20report,unacceptable%20level%20of%20customer%20dissatisfaction; *see also Knowledge-Based Authentication Weaknesses,* Identity Management Institute Center for Identity Governance Blog, https://identitymanagementinstitute.org/knowledge-based-authentication-weaknesses/.
[57] 2022 *Voice Intelligence & Security Report: Let the Right Voice In* at 6, https://go.pindrop.com/resources/report/2022-voice-intelligence-and-security-report/#:~:text=2022%20Voice%20Intelligence%20%26%20Security%20Report,according%20to%20this%20year's%20report.
[58] *Id.* at 7.
[59] *DATA PROTECTION Federal Agencies Need to Strengthen Online Identity Verification Processes* (GAO-19-288 May 2019) at i, https://www.gao.gov/assets/gao-19-288.pdf.
[60] *Id.* at 29.
[61] 2022 *Voice Intelligence & Security Report: Let the Right Voice In* at 6, https://go.pindrop.com/resources/report/2022-voice-intelligence-and-security-report/#:~:text=2022%20Voice%20Intelligence%20%26%20Security%20Report,according%20to%20this%20year's%20report.
[62] G.S. 10B-134.21(a)(3).
[63] G.S. 10B-134.19(e)(2).

large amounts of stolen personal data being widely available on the dark web to anyone wishing to pay modest amounts, leading to the risk of a false acceptance. An incomplete database of acceptable credentials would lead to a false rejection during the credential analysis step, even if the credential otherwise was an acceptable form of identification.

The Secretary wishes to understand false acceptance and rejection rates for various identity proofing technologies, and how rulemaking can ensure identity verification is configured to limit the risks of false acceptance and rejection.

Question D.1. What is the effectiveness of the various identity verification technologies now available, *i.e.,* do the various identity verification technologies have established false acceptance and false denial rates and, if so, what are they? If you are aware of any studies describing the effectiveness of any of these technologies, please provide the information necessary for the Secretary to access them.

Question D.1.a. Are there industry standards for acceptable false acceptance and rejection rates for any identity verification technologies? What are they?

Question D.1.b. How should these rates be ascertained and verified? May the Secretary depend upon vendor certifications, or should the rates be verified by outside auditors?

Question D.1.c. Are there false acceptance and false denial rates that are acceptable to those who will depend upon RENPs to positively identify a principal? If there are acceptable rates, what are they? Do the rates vary among stakeholders (*i.e.,* do mortgage closings need a different accuracy rate than will signings or participants in judicial proceedings?)

Question D.2. What constitutes information that is sufficiently "personal" that it will aid in the positive identification of a person and can be used in the context of a REN? Is such information historical, biographic, locational, biometric, or something else?

Question D.2.a. What type of personal information is necessary to create confidence that the person providing that information is who they say they are?

Question D.2.b. If personal information is widely known to persons other than the RLP, how can such information be used to provide confidence that the identity of the RLP has been properly proofed and has not been fraudulently assumed for the purposes of the REN?

Question D.3. With regard to "data sources":

Question D.3.a. If the Secretary has the authority to ask the third-party vendor to identify the public and proprietary sources used in identity proofing, may the third-party vendor designate that information as a trade secret in accordance with the NC Trade Secrets and Public Records Acts[64]? If yes, explain the basis for your response, and please provide citations.

Question D.3.b. How accurate must the databases and processes used to compare the data against information provided by the RLP be in order to be a permissible form of identity proofing?

Question D.3.b.1. What are the measures of accuracy to evaluate the databases and processes?

Question D.3.b.2. Should the claims of database and process accuracy be ascertained by audit, independent third parties, or vendor self-verification?

Question D.4. Please provide information about the various types of current identity proofing technologies having wide acceptance. Include:

Question D.4.a. An explanation of how the technologies work.

Question D.4.b. Are there specific terms commonly used to identify and describe these technologies? If yes, what are they?

Question D.4.c. Are these technologies typically open-source or are they typically the intellectual property of individuals or business entities? Please explain.

Question D.4.d. Are there common features of these technologies that should be required in the rules?

Question D.4.e. Are there laws, rules, regulations, industry or other standards that define the "identity proofing" process or otherwise apply to these technologies? If yes, what are they? Be specific.

Question D.4.f. What are the minimum identity proofing requirements that satisfy the RENA purpose of preventing fraud?

Question D.4.g. Should the Secretary limit the public and proprietary sources used in identity proofing to

[64] G.S. 66-152 *et seq.;* G.S. 132-1.2(1).

those for which affected RLPs have a right to review and correct or comment on the information? Please explain your response and provide citations as appropriate.

Question D.4.h. Is there a minimum standard for the quality of personal information used or the number of sources or questions from sources that the identity proofing technology would use? Please explain.

Question D.4.h.1. If yes, what is that minimum standard?

Question D.4.h.2. What type personal information is more reliable than other information and also available for use in identity proofing?

Question D.4.i. With regard to identity proofing technology,

Question D.4.i.1. Should the rules set a minimum standard in terms of the number or type of:

- Personal information items provided by the RLP that are checked against the public or proprietary source?
- Number of sources checked?
- Whether the sources checked include both public and proprietary sources?
- Number of correct matches of facts obtained from the sources?
- Number of correct answers to questions based upon facts obtained from the sources?
- Number of rounds that an RLP may attempt before rejection?
- Other?

Question D.4.i.2. If so, please provide rationale, authority, and/or instance where it is used.

Question D.4.j. If the identity proofing technology does not rely on asking the RLP questions and matching the answers to information in public and proprietary sources, how can the RLP find out that the information relied upon by the technology is incorrect? How would the RLP challenge that information or ask for another chance to prove the RLP's identity is correct?

Question D.4.k. Are there questions that the technology should be barred from using for purposes of identity proofing?

- If yes, what are those questions?
- What is the legal basis for such a bar on questions?

Question D.4.l. How else might the Secretary's rules ensure against false rejection or acceptance? Please explain.

D.5. Certain government agencies may issue identification with data points required by G.S. 10B-2(22) that can be read only by specialized hardware. Examples include mobile drivers' licenses and military common access card identification, which use embedded data technology.

Question D.5.a. Is there sufficient momentum for personal identification with embedded data to warrant providing for it through rule making at this time?

Question D.5.b. What provisions should be made?

D.6. With regard to the credential analysis process,

Question D.6.a. Are there laws, rules, regulations, industry or other standards that govern, define or describe the operation and accuracy of the credential analysis process? If yes, what are they? Please be specific.

Question D.6.b. Are there industry or other standards that govern, define or describe the operation of the credential analysis process? If yes, what are they, please be specific.

Question D.6.c. What minimum characteristics and security features should the rules require be identified and analyzed? Salient characteristics and security features may vary widely from state to state and nation to nation, and also over the course of time.

Question D.6.d.1. Should the rules establish minimum characteristics and security features that must be present in any identification document presented without regard to standards set by the issuing entity?

Question D.6.d.2. Or is it enough to rely upon the standards established by the issuer, even if those standards become outdated and susceptible to fraudulent creation, distribution, or usage?

Question D.6.d.3. Should the rules require analysis of the most robust security features – for example, reading the radio frequency identification chip that is embedded in US Passport Cards?

Credential analysis of the "characteristics and security features" of each identification document would at a minimum require the technology to:

- Determine if the identity document is an acceptable form of identification.
- Determine if the document is validly issued.
- Determine if the document is current.
- Analyze for correctness of the placement of the elements of the identity document on the document (*e.g.*, where the photograph or physical description of the individual appears).
- Analyze whether the expected security features of the identity document are present and correct.

Question D.7. Please identify any other steps that should be taken as part of the credential analysis and explain the basis for their inclusion.

Question D.8. How does the credential analysis process work, and what minimum standards should be adopted to ensure reliability of credential analysis technologies?

Question D.8.a. Does the credential analysis process involve comparison of data on the identity document to public or other data sources?

E. Security Governance, Chief Information Security Officers and Their Equivalents

RENA requires that an application from a platform include "explanations regarding security governance and the designation of a chief security officer or its equivalent."[65] RENA does not define "security governance," CISO or the equivalent. The Secretary must include definitions or explanations of these terms. The role and responsibilities of a CISO, the qualifications to be a CISO, and the relationship of the CISO to the applicant's IT security governance must be clearly articulated in order to establish whether the statutory requirements are met, and whether an individual may be considered the equivalent of a CISO. The designated CISO or equivalent must be directly involved in "operation, management or control" of the technology and therefore will be subject to a background check and criminal record check.

Question E.1. What are the minimum attributes of an effective "IT security governance"?

Question E.2. Are there laws, rules, regulations, industry, or other standards the Secretary should review that define:

- Security governance?
- Chief information security officer?
- Equivalent of a CISO?

If yes, please provide citations.

Question E.3. Are there standards or minimum qualifications for persons filling the role of CISO that will help determine whether a person is "equivalent" to a CISO? If yes, what is the source of the standards? Please be specific.

Question E.3.a. If yes, are there minimum education, training, and experience requirements for persons filling that role and what are they?

Question E.3.b. If there are no standards or minimum qualifications, what criteria can be used to determine whether a person with the title of CISO or its equivalent is qualified?

Question E.4. What minimum physical security standards should be required, if any, to assure adequate IT security governance?

Question E.5. Are there laws, rules, regulations, or industry or other standards that set out minimum elements of software, hardware, and cloud-solution security governance for a technology provider?

Question E.5.a. If yes, what are they? Please be specific.

Question E.5.b. If there are preferred versions of such minimum standards, please explain and be specific.

Question E.5.c. If there are versions that you consider, for whatever reason, to be less desirable, less up to date, etc., please explain. Be specific.

[65] G.S. § 10B-134.19(c)(3).

Question E.6. Are there standard or uniform means of measuring the effectiveness of an IT provider's security governance?

Question E.6.a. If yes, what are they? Please provide citations.

Question E.6.b. Are there means and methods of measuring IT security governance effectiveness that are preferred because of accuracy and thoroughness? If yes, please explain.

Question E.6.c. Are there means and methods of measuring IT security governance effectiveness that should be evaluated in connection with assuring the security of the communication platforms and identity verification technologies? If yes, please explain.

Question E.6.d. Is there IT security governance terminology or commonly understood terms that the Secretary should be aware of and use when requesting additional information or proof of IT security governance effectiveness? Avoid using? What are they?

F. Geolocation

RENA requires that the communication technology be capable of geolocating the RLP to corroborate the RLP's location[66] so that the RENP may verify the RLP's location before performing the REN act.[67] In order to meet these requirements, the platform applicant must specify "the proposed technology to address "geolocation requirements."[68]

"Geolocation" is not defined in RENA. "Geolocation information" is listed in the State's Student Online Privacy Protection law but is defined neither there nor in related rules.[69] The word "geolocation" appeared in several failed bills in the 2021-2022 session of the General Assembly, including one that included this definition for "precise geolocation data":

Information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms that directly identify the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.[70]

Both the North Carolina Education Lottery and the Eastern Band of Cherokee Indians use geolocation to ensure that customers are within the geographic boundaries authorized by law.[71]

Geolocation of an individual may be general, somewhat specific, specific, or exceptionally precise. For example, general geolocation might confirm that the person is in the United States. Somewhat specific geolocation might confirm that the person is in a specific state or U.S. territory. Specific geolocation might confirm that the person is located in a particular town or even at a specific address. RENA does not specify the level of precision that the Secretary should require in confirming the location of an RLP. At a minimum, geolocation of an RLP must in real-time:

- Identify whether the RLP is at that moment located within one of the 50 states, the District of Columbia, or a U.S. territory.

- Identify whether the RLP is at that moment located within the official boundaries of a United States military installation.

---

[66] G.S. 10B-134.5(a)(7).
[64] G.S. 10B-134.9(a)(6).
[68] G.S. 10B-134.19(c)(3).
[69] G.S. 115C-401.2(a)(1)c.29.
[70] Consumer Privacy Act, S. 569, Section 2 § 75-70(a)(20) at 2 (2021-22 N.C. General Assembly Session).
[71] Frequently Asked Questions: Online Play: Geo Location, https://nclottery.com/FAQOnlinePlay (Last viewed Mar. 17, 2023); Second Amended & Restated Tribal - State Compact Between the Eastern Band of Cherokee Indians and the State of North Carolina at 12 para. 20 (2020), https://www.bia.gov/sites/default/files/dup/assets/as-ia/oig/pdf/508%20Compliant%202021.03.02%20Eastern%20Band%20Cherokee%20Tribal%20State%20Gaming%20Compact%20Amendment.pdf.

- Identify whether the RLP is at that moment located within the official boundaries of a United States embassy, consulate, or diplomatic mission.

Question F.1. If there are laws, rules, regulations, industry, or other standards that define geolocation, please provide citations.

Question F.2. How precise must the geolocation be in order to meet the criteria of RENA and to prevent fraud?

Question F.3. If there are laws, rules, regulations, industry or other standards that clarify the different levels of specificity of geolocation please provide citations.

Question F.4. How precisely can various devices (*e.g.*, handheld mobile devices, laptops, desktops and the like) and connections (*e.g.,* direct connection to internet service provider, network connection, VPN connection) geolocate the position of the device and how reliable is the technology in general and each device specifically?

Question F.4.a. Does the geolocation precision vary by device, by type of connection, or by software?

RENA requires that the RLP's location be confirmed by the RENA technology provider's geolocation technology. This would seem to bar the RENP from accepting the RLP's explanation of differences between the RLP's stated location and that determined by geolocation technology.

Question F.5. If the location stated by the RLP is not confirmed by the geolocation by the RENA technology provider, must the REN act be terminated? Or does the RENP have the discretion to proceed to perform the REN act even though the location cannot be verified by the geolocation technology?

"Compliance grade" geolocation involves more complex systems than merely checking an IP address or GPS address against that stated by the RLP. "Two types of data can be collected—active user/device-based information and passive server-based lookup/data correlation—and then cross-referenced against each other to create the most accurate result."[72] Just as multi-factor authentication for user identities is gradually becoming the norm, geolocation that involves use of more than one method of comparing geolocation results may be needed to both ensure geolocation accuracy and prevent fraud. The Secretary invites comment on the following questions:

Question F.6. Is there a minimum number of cross-references of geolocation that is acceptable? Is cross-reference the correct term? If not, what word or phrase should the Secretary use?

Question F.6.a. If yes, please explain, and provide citations where available.

Question F.6.b. If no, please explain, and provide citations where available.

Question F.7. Are there government, industry, or other standards regarding the minimum acceptable and optimal levels of geolocation cross-checks, in relation to both accuracy and fraud detection and prevention?

Question F.7.a. If yes, please provide citations.

Question F.7.b. If, among the standards you cite, you have a preference, please explain.

Question F.7.c. If, among the standards you cite there are any that you think the Secretary should not use, please explain.

Question F.8. Are there government or third-party certifying organizations that set standards for accuracy of geolocation software and services (*e.g.,* NIST or ISO)?

Question F.8.a. If yes, please provide their names and links to their websites.

Question F.8.b. If yes, please provide the title of the geolocation-related standards and a link to them.

[72] Betsie Estes, *Geolocation--The Risk and Benefits of a Trending Technology* at 1 (Sept. 26, 2016), https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/geolocationthe-risk-and-benefits-of-a-trending-technology.

Question F.9. Are there government or third-party certifying organizations that set standards for use of geolocation software and services in fraud prevention and detection (*e.g.,* NIST or ISO)?

Question F.9.a. If yes, please provide their names and links to their websites.

Question F.9.b. If yes, please provide the title of the geolocation-related standards and a link to them.

G. IT Security Standards and Features, and Performance Standards

The Cybersecurity Maturity Model Certification (CMMC) program published by NIST is an assessment framework and assessor certification program designed to increase trust in measures of compliance with a variety of IT standards. CCMC is specifically focused on the handling of controlled unclassified information by U.S. Department of Defense vendors. It is based on the existing NIST SP 800-171 controls.

NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) is widely used in commercial and local and state government settings. There is significant overlap with NIST 800-171, but both provide frameworks which can be used in self-assessment or in third party assessments.

Question G. What mechanism would achieve the appropriate balance between assuring public confidence in the security and integrity of technologies used by an RENP to perform an REN while also allowing IT providers the flexibility to develop innovative products in support of REN (*e.g.*, outside security governance)?

Question G.1. Is the CMMC program a viable standard in the REN context? If not, why not?

Question G.2. Is NIST 800-53 a viable standard in the REN context? If not, why not?

Question G.3. Is there some other standard that should be incorporated? If so, please provide particulars.