27 NCAC 01D .3305 STANDARDS FOR CERTIFICATION AS A SPECIALIST IN PRIVACY AND INFORMATION SECURITY LAW

Each applicant for certification as a specialist in privacy and information security law shall meet the minimum standards set forth in Rule .1720 of this subchapter. In addition, each applicant shall meet following standards for certification in privacy and information security law:

(a) Licensure and Practice - An applicant shall be licensed and in good standing to practice law in North Carolina as of the date of application. An applicant shall continue to be licensed and in good standing to practice law in North Carolina during the period of certification.

(b) Substantial Involvement - An applicant shall affirm to the board that the applicant has experience through substantial involvement in privacy and information security law.

(1) Substantial involvement shall mean that during the five years immediately preceding the application, the applicant devoted an average of at least 400 hours a year to the practice of privacy and information security law but not less than 300 hours in any one year.

(2) Practice shall mean substantive legal work in privacy and information security law done primarily for the purpose of providing legal advice or representation, including the activities described in paragraph (3), or a practice equivalent as described in paragraph (4).

(3) Substantive legal work in privacy and information security law includes, but is not limited to, representation on compliance, transactions and litigation relative to the laws that regulate the collection, storage, sharing, monetization, security, disposal, and permissible uses of personal or confidential information about individuals, businesses, and organizations. Practice in this specialty requires the application of information technology principles including current data security concepts and best practices. Legal work in the specialty includes, but is not limited to, knowledge and application of the following: data breach response laws, data security laws, and data disposal laws; unauthorized access to information systems, such as password theft, hacking, and wiretapping, including the Stored Communications Act, the Wiretap Act, and other anti-interception laws; cyber security mandates; website privacy policies and practices, including the Children's Online Privacy Protection Act (COPPA); electronic signatures and records, including the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) and the Uniform Electronic Transactions Act (UETA); e-commerce laws and contractual legal frameworks related to privacy and data security such as Payment Card Industry Data Security Standards (PCI-DSS) and the NACHA rules; direct marketing, including the CAN-SPAM Act, Do-Not-Call, and Do-Not-Fax laws; international privacy compliance, including the European Union data protection requirements; social media policies and regulatory enforcement of privacy-related concerns pertaining to the same; financial privacy, including the Gramm-Leach-Bliley Act, the Financial Privacy Act, the Bank Secrecy Act, and other federal and state financial laws, and the regulations of the federal financial regulators including the SEC, CFPB, and FinCEN; unauthorized transaction and fraudulent funds transfer laws, including the Electronic Funds Transfer Act and Regulation E, as well as the Uniform Commercial Code; credit reporting laws and other "background check" laws, including the Fair Credit Reporting Act; identity theft laws, including the North Carolina Identity Theft Protection Act and the Federal Trade Commission's "Red Flags" regulations; health information privacy, including the Health Information Portability and Accountability Act (HIPAA); educational privacy, including the Family Educational Rights and Privacy Act (FERPA) and state laws governing student privacy and education technology; employment privacy law; and privacy torts.

(4) "Practice equivalent" shall mean:

(A) Full-time employment as a compliance officer for a business or organization for one year or more during the five years prior to application may be substituted for an equivalent number of the years of experience necessary to meet the five-year requirement set forth in Rule .3305(b)(1) if at least 25% of the applicant's work was devoted to privacy and information security implementation.

(B) Service as a law professor concentrating in the teaching of privacy and information security law for one year or more during the five years prior to application may be substituted for an equivalent number of years of experience necessary to meet the five-year requirement set forth in Rule .3305(b)(1);

(c) Continuing Legal Education - To be certified as a specialist in privacy and information security law, an applicant must have earned no less than 36 hours of accredited continuing legal education credits in privacy and

information security law and related fields during the three years preceding application. The 36 hours must include at least 18 hours in privacy and information security law; the remaining 18 hours may be in related-field CLE or technical (non-legal) continuing education (CE). At least six credits each year must be earned in privacy and information security law. Privacy and information security law CLE includes but is not limited to courses on the subjects identified in Rule .3302 and Rule .3305(b)(3) of this subchapter. A list of the topics that qualify as related-field CLE and technical CE shall be maintained by the board on its official website.

(d) Peer Review - An applicant must make a satisfactory showing of qualification through peer review. An applicant must provide the names of ten lawyers or judges who are familiar with the competence and qualification of the applicant in the specialty field to serve as references for the applicant. Completed peer reference forms must be received from at least five of the references. All references must be licensed and in good standing to practice law in North Carolina or another jurisdiction in the United States; however, no more than five references may be licensed in another jurisdiction. References with legal or judicial experience in privacy and information security law are preferred. An applicant consents to confidential inquiry by the board or the specialty committee to the submitted references and other persons concerning the applicant's competence and qualification.

(1) A reference may not be related by blood or marriage to the applicant nor may the reference be a colleague at the applicant's place of employment at the time of the application. A lawyer who is in-house counsel for an entity that is the applicant's client may serve as a reference.

(2) Peer review shall be given on standardized forms provided by the board to each reference. These forms shall be returned to the board and forwarded by the board to the specialty committee.

(e) Examination - An applicant must pass a written examination designed to demonstrate sufficient knowledge, skills, and proficiency in the field of privacy and information security law to justify the representation of special competence to the legal profession and the public.

(1) Terms - The examination shall be given at least once a year in written form and shall be administered and graded uniformly by the specialty committee or by an organization determined by the board to be qualified to test applicants in privacy and information security law.

(2) Subject Matter - The examination shall test the applicant's knowledge and application of privacy and information security law.

History Note: *Authority G.S. 84-23;*
Approved by the Supreme Court September 28, 2017;
Amendments Approved by the Supreme Court: December 14, 2021.