The State Bar of California

**Task Force on Access Through Innovation of Legal Services – Subcommittee on Unauthorized Practice of Law and Artificial Intelligence**

| | |
|---|---|
| To: | Subcommittee on Unauthorized Practice of Law and Artificial Intelligence |
| From: | Heather Morse |
| Date: | March 25, 2019 |
| Re: | B.3. What experience do law firms have and what feedback can they provide regarding security standards that they are implementing and/or have been asked by clients to implement? |

I spoke to several of my peers across the country, and here are the security standards law firms are currently being asked to implement by clients:

- ISO 17799 certification
- ISO 27001 certification
- BS 7799 standard certification
- HITRUST - The **Health Information Trust Alliance**, or **HITRUST**, is a privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework (CSF) that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data. The CSF includes a prescriptive set of controls that seek to harmonize the requirements of multiple regulations and standards.

Additional requests from a current Request for Proposal (RFP) from a financial institution:

- The organization shall establish information security policies, standards, and procedures which are reviewed and management-approved at least annually and applicable to the entire organization. Policies shall be based on a generally accepted framework, such as NIST, ISO 27001, or COBIT, and include but not be limited to, the following topics areas:

  - identification, authentication and access control
  - change and configuration management
  - information system maintenance
  - system and information integrity
  - system and communications protection
  - malicious code protection
  - data loss prevention
  - audit and accountability
  - acceptable use
  - compliance
  - security assessment and authorization
  - risk assessment
  - human resources
  - third party security
  - data stewardship, with assigned responsibilities defined, documented, and communicated.

- The organization shall follow procedures to comply with PII/PHI data breach notification legislation in all applicable jurisdictions.

- **Application Development Security Framework (ADSF)**
  In the event a third-party hosts (a) Internet-facing web or mobile applications, or (b) web or mobile applications accessible by [financial institution] associates that utilize web technology and handle non-public data, such third party must allow, at the request of [financial institution], an Application Development Security Framework (ADSF) vulnerability assessment (e.g., ethical hacking). Such vulnerability assessment shall be conducted in a non-production environment with production equivalent security controls and with prior notice to the third party. All new or significantly changed web and/or mobile applications that are (a) Internet-facing or (b) accessible by [financial institution] employees that utilize web technology and handle non-public data, must have an ADSF vulnerability assessment (e.g., ethical hacking) prior to production use. (e.g., "go live" date). The [financial institution] Global Information Security (GIS) ADSF engagement process will determine the level of assessment required. In accordance with the ADSF high risk application program, third party applications which are Internet-facing and applications qualified as "high risk" by [financial institution] that utilize web technology are to be assessed minimally on a 12 month basis.

- **Payment Card Industry Data Security Standards (PCI DSS)**
  To the extent a third party will store, process, transmit or otherwise access or possess cardholder data in connection with the services provided to [financial institution], the third party shall have an obligation to secure cardholder data and to adhere to the Payment Card Industry Data Security Standard (PCI DSS) for the protection of cardholder data. The Attestation of Compliance (AOC) document must be signed off by a Qualified Security Assessor (QSA) within the last 12 months. The third party shall be responsible for the security of cardholder data in the possession or control of any subcontractors it engages to perform services pursuant to its agreement with [financial institution]. Such subcontractors must be identified to and approved by [financial institution] in writing prior to sharing cardholder data with the subcontractor. In support of this obligation, the third party shall provide appropriate documentation to demonstrate compliance with applicable PCI DSS requirements by third party and all subcontractors.

**Validated Cryptology Algorithms** - Sensitive data is encrypted with a technology solution validated by the National Institute of Standards and Technology (NIST) and contained in the FIPS 140-2 publication. More information on the Cryptographic Module Validation Program (CMVP) can be found at http://www.nist.gov/cmvp. FIPS 140-2 defines four levels of increasing security, simply named "Level 1" to "Level 4". The minimum allowable security level for Company encryption is Level 1.