**Appendix A**

Current Process for Mandatory Independent Security Assessments of California Agencies

Use this as a process model for CCPA risk assessments, based on output from CCPA cybersecurity audits:

Graphical user interface, diagram, application

Description automatically generated

1. Entities begin the ISA process when they receive a formal notification letter from California Department of Technology (CDT) Office of Information Security (OIS) advising them that it is their year to undergo an ISA.
   1. Entities can seek approval to undergo a commercial, 3rd party ISA by attaching a copy of the proposed Statement of Work for the contract to the ISA Compliance Certification Form. The completed ISA report must meet the ISA Criteria\* EXACTLY and follow the SAME FORMAT.

***Note:*** All businesses and organization registered with the California Secretary of State should receive a “Welcome Packet” promoting awareness of the new CCPA Regulations and Resource Guide to help them comply with the Regulations and additional reporting requirements.

***Note:*** Businesses and Consumers can use an online service to determine which classification status applies to the entity as 1) CCPA-Exempt; 2) CCPA-Covered; 3) Data Brokers; 4) Large Businesses; 5) High-Risk Processors. This tool also informs the user which obligations apply to each entity class. For a CCPA-Exempt entity, it would state the entity has no legal obligations under the CCPA, and advise that a consumer may reasonably expect them to comply with the CCPA unless told otherwise.

***Note:*** All CCPA-covered entities must complete a Risk Assessment Questionnaire. This is designed to confirm or address any discrepancies in their classification status and assess their awareness of the CCPA through simple tests anyone could conduct. For example, all CCPA-covered entities must have a published privacy policy, but if the policy predates the passage of the new CPRA-amended CCPA Regulations, it’s more likely than not that they are non-compliant and recommend they consult the Resource Guide.

***Note:*** All CCPA-covered entities classified as Data Brokers, Businesses Collecting Large Amounts of Personal Information, and High-Risk Processors would be required to fill out an Initial Asset Count Worksheet. This worksheet is designed to identify assets critical to the scope of an audit. It includes registered domains, websites, IoT devices, brand names, subsidiaries, parent companies. It would also include estimated counts of employees, consumer profiles, service providers, contractors, and third parties involved in collecting or processing PI. Counting the average number of sensitive data elements and attributes stored or processed helps the Agency designate which entities meet the criteria for mandatory risk assessments and audits.

***Note:*** Audits and assessments are verified through testing controls, and the controls which are tested must be sampled from a finite population. Without making the entire inventory of system asset public information, input from consumers and other agencies can use other sources to verify or refute the scope of assets tested.

1. Entities begin the ISA scheduling process by completing the Initial Asset Count Worksheet. (Appendix A)
2. Create the ISA Case from the CDT IT Services Portal catalog within 30 days of the date of official notification.
3. Receive Confirmation of ISA Dates and Cost Estimate/Work Authorization and return the signed CE/WA to the Cyber Network Defense (CND) Engagement Manager who officially schedules the entity’s assessment dates.
4. Entity receives a copy of the CND Preparedness Guide from the CND Engagement Manager with an email confirming the schedule for their ISA. The Preparedness Guide will enable the entity to be as prepared as possible for CND’s arrival on site and to ensure the best possible outcome and benefits from the ISA.

The ISA is conducted using a two-team approach. The Risk Analysis (RA) team conducts (BLUE TEAM) tasks related to the defensive controls assessed (task sections 10-15). The Penetration Test (Pen Test) team conducts (RED TEAM) activities related to the offensive simulation operations portion of the assessment (task sections 16-17).

If the Pen Test Team detects a Significant Risk, it will initiate a “Hard Pause” if delayed disclosure is likely to result in network compromise by a real-world threat actor. The Pen Test Team provides the Entity Liason with information pertaining to the detected risk, impacted host(s), and recommended course of action to reduce the risk to the enterprise.

If the CND detects the potential presence of Illegal Activity (external threat actor compromise, insider threat activities, etc.) the ISA will initiate a “Hard Stop”. The Pen Test Team, working with the entity’s management team, perform the required initial reporting to Cal-CSIRS as well as facilitate any interim evidence preservation process for red team actions.

Areas within the current ISA include host vulnerability assessments, firewall analysis, host hardening analysis, phishing susceptibility, network penetration testing, and snap-shot analysis of network traffic for signs of threat actor compromise.

***Note:*** This proposal is not suggesting that CMD conducts all risk assessments, but that standards and guidelines for third-party assessors be aligned with CMD standards to a reasonable degree.