**Appendix C**

Proposed Control Set for Initial Risk Assessment Summaries for Identifying High-risk Entities.

***Proposal*** Use this smaller subset of common controls from NIST, ISO, CIS, and OWASP to establish a minimum standard nearly all businesses can meet. If more stringent standards are needed due to significantly greater risk exposure or harm, they can be layered on top of the baseline, much like PCI-DSS or HITRUST is structured. This control subset is documented in this Excel Workbook, published in my public data catalog accessible from this link:

<https://query.data.world/s/iohi7b7aao4bb5on6bjvifvwfbj3le?dws=00000>

***Note:*** The methodology I used to create a smaller subset was:

1) select the greatest number of common controls from all standards

2) select the controls most relevant to CCPA test cases and mandated cybersecurity audits and assessments.

***Note:*** NIST 800-53r4 is the current standard for California Office Information Security. This proposed control set uses Revision 5 which incorporates many controls from the Privacy Framework and Cybersecurity Framework for Improving Critical Infrastructure. It represents a baseline canonical model, which all other standard control frameworks are mapped to.

**National Institute of Standards and Technology Special Publication 800-53, Revision 5**

<https://doi.org/10.6028/NIST.SP.800-53r5>

*This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.*