December 3, 2019

Attorney General Xavier Becerra
Office of the Attorney General
State of California Department of Justice

Subject: CCPA and Minimum Reasonable Information Security Practices

Dear Mr. Attorney General:

I speak to you as the founder and President of a California nonprofit, *SecureTheVillage*. We are a community of information security practitioners; IT vendors and MSPs; attorneys with a practice in cyber; cyber-investigators; insurance and risk management professionals; law enforcement, including the FBI, Secret Service, and both the Los Angeles County and Orange County District Attorney's Office; and others. In addition to our base in Los Angeles, our community extends to Orange County and Sacramento.

The experience and expertise of our organization's members runs deep. Speaking personally, I entered the field of computer security in 1980 as a young Ph.D. in mathematical logic from The University of Michigan. In those early years, I was privileged to work securing advanced technology systems for the White House, Strategic Air Command, NASA and other national assets. Seventeen years ago, I co-founded an information security management firm, Citadel Information Group, to assist mid-market and smaller organizations manage their information security needs. In the 9 years prior to founding SecureTheVillage in 2015, I served as President of the Los Angeles Chapter of the *Information Systems Security Association*.

I speak to you today regarding the California Consumer Privacy Act (CCPA) *Right of Compensation* to consumers in the event of a data breach *except when the breached business maintains "reasonable security procedures and practices appropriate to the nature of the information being protected."*

As has been widely discussed, there is a great deal of uncertainty as to exactly what "*reasonable security procedures and practices*" is to mean.

In response to this uncertainty, *SecureTheVillage* has developed and published—as a free public service—a set of *Minimum Reasonable Information Security Management Practices*. [1]

[1] See https://mrsp.securethevillage.org/.

For the reasons described below, we invite you to use our *Minimum Reasonable Information Security Management Practices* in assisting California establish appropriate reasonability requirements for organizations to follow in complying with CCPA and other information security management obligations.

SecureTheVillage views these *minimum reasonable* practices as so basic to the responsibility of securing private consumer information that a failure to implement them should be considered *prima facie* evidence that an organization's information security procedures and practices are not reasonable. We developed them to be *commercially reasonable* and *reasonably achievable* for any company subject to CCPA.

It is important to note that we are not saying that an organization meeting these minimum practices has reasonable practices. To cite one example, the "reasonability" requirement for a large telecommunication or Internet Service Provider is considerably more than our suggested minimum. And even a company that meets our minimum standards might still not have reasonable standards *appropriate to the nature of the information being protected*. *Our suggested minimum is designed to establish the floor, not set the bar*.

SecureTheVillage's *Minimum Reasonable Information Security Management Practices* are based upon other existing information security standards. These include:

1. The NIST Cybersecurity Framework
2. The International Standards Organization ISO 27001 family, Information Security Management
3. The Center for Internet Security's Critical Security Controls [CIS-20]
4. The New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies
5. NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

SecureTheVillage's *Minimum Reasonable Information Security Management Practices* have nine basic elements.

1. Information Security Management
2. Information Security Subject Matter Expertise
3. Security Management of Sensitive and Private Information
4. Security Awareness Training / Culture Change (SecureTheHuman)
5. Security Management of the IT Interface: Use of CIS-20 Critical Security Controls [2]
6. Security Management of the IT Infrastructure: Use of CIS-20 Critical Security Controls

[2] At the present time, our incorporation of the CIS-20 is based upon the Center's Version 6 controls. We will be upgrading our minimum to the newer CIS Version 7 controls later this year or early in 2020.

7. Third-Party Security Assurance
8. Information Resilience
9. Information Security Governance

A natural question is why not use the CIS-20 as the standard of *reasonability*. After all, the CIS-20 was identified by then Attorney General Kamala Harris in the California 2016 Data Breach Report as providing a minimum *reasonableness* standard.

SecureTheVillage believes the CIS-20 standards are – in part - too weak to be reasonable and – in part - too strong.

We believe the CIS-20 is too weak to meet the *reasonableness* threshold in that they do not naturally encompass the aspects of information security management that lie outside of managing the technology infrastructure: Organizational management, Governance, Leadership, Training, Cultural adaptation, etc. We believe these elements — included in ISO 27001, the NIST Framework, 23NYCRR 500 — need to be included in any reasonable definition of *reasonableness.*

Likewise, we believe some of the CIS-20 controls are not commercially reasonable for smaller organizations which might be subject to the CCPA. Penetration testing is a good example as it is not cost-effective for smaller companies. These companies can get considerably more risk-driven value from network vulnerability scanning and phishing simulations.

For more information, we invite you to review the details of SecureTheVillage's *Minimum Reasonable Information Security Management Practices*. They are available at the link noted above and also accessible from the Resources Section on our website: www.SecureTheVillage.org.

It would be my pleasure to meet with staff to discuss further how SecureTheVillage's *Minimum Reasonable Information Security Management Practices* supports California's need for a well-defined standard for *reasonable security practices*.

Thank you for your consideration. Thank you as well for your leadership in helping California find the right judicial answers to meet the challenges of cyber-crime, cyber privacy and information security.

Sincerely,

Stan Stahl, Ph.D.
SecureTheVillage
Founder and President
Stan@SecureTheVillage.org
323-428-0441