

The Sedona Conference

Commentary on a Reasonable Security Test

(September 2020 Public Comment Version)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11) developed this *Commentary* to address what “legal test” a court or other adjudicative body should apply in a situation where a party has, or is alleged to have, a legal obligation to provide “reasonable security” for personal information, and the issue is whether the party in question has met that legal obligation.

The *Commentary* proposes a reasonable security test that is designed to be consistent with models for determining “reasonableness” that have been used in various other contexts by courts, in legislative and regulatory oversight, and in information security control frameworks. All of these regimes use a form of risk analysis to balance cost and benefit. The proposed test provides a practical method for expressing cost/benefit analysis that can be applied in data security regulatory actions, to litigation, and to information security practitioners using their current evaluation techniques. The *Commentary* also explains how the analysis should apply in the data security context. Because the test is rooted in commonly held principles, the drafters believe it offers methods for deriving reasonableness that are familiar to all interested parties. But it should be noted that depending on their text, individual laws or rules that require reasonable security might require use of a different analysis.

The *Commentary* begins with a brief summary of the importance of having a test, the reasoning behind a cost/benefit approach for the test, and what issues the test does not address. Part I sets out the proposed test and the explanation of how it is applied. Part II provides review and analysis of existing resources that offer guidance on how “reasonable security” has been defined and applied to date and explains how they bear upon the test. It includes a summary review of statutes and regulations that require organizations to provide reasonable security with respect to personal information, decisions of courts and other administrative tribunals with respect to the same, applicable industry standards, and marketplace information. Following this discussion, the *Commentary* identifies those items that are not included in the proposed test (also referenced in the Introduction section) and concludes with a discussion regarding the importance of flexibility.

The full text of The Sedona Conference *Commentary on a Reasonable Security Test*, Public Comment Version, is available free for individual download from The Sedona Conference website at

https://thesedonaconference.org/publication/Commentary_on_Reasonable_Security_Test.

© 2020 The Sedona Conference. Reprinted courtesy of The Sedona Conference.