While I appreciate all the work which has gone into the preparation of this "Report to the President on Enhancing Resilience of the Internet …" (CSRC report), dated January 5, 2018, I have serious reservations about its conclusions. I will mention just three, but there are more.

(1) Approach Too Technical: The approach taken in the CSRC report is predominantly technical, and America's technical environment is shaped by morals, ethics, laws, regulations, social expectations, business contracts, and the like. These "soft factors" are not sufficiently addressed in the CSRC report, but are in fact causative of the technical ecosystem we face today. For example, the laws defining what is criminal and what is not, laws that clearly define criminal acts, need to be standardized across nations, because the Internet is now worldwide. We do not even have a standardized way to talk about these things right now. If we cannot talk about them using a common language, then we will not be able to think about them in an effective way that is going to bring about adequate security and privacy. For further discussion about the need to reform the underlying legal system, see the article entitled: "A Simple Appeal to Common Sense: Why the Current Regulatory Regime for Information Security & Privacy Doesn't Work, and Can't Be Made to Work," by Wood, Rogers, and Poore (December 2017, ISSA Journal).

http://www.issa.org/?page=ISSAJournal

(2) System Reconceptualization Needed: The approach taken in the CSRC report is basically more of the same. It assumes that we have the tools we need, we have the correct laws, we just need more of certain things like cooperation, training, etc. The above-mentioned article (see link) sets out nine explicit reasons why that "just do more of the same stuff" approach cannot work. We need to rethink the whole system. Consider the economics of attackers and defenders. The economic investment made by an attacker can in many cases be considerably less than the economic investment made by a defender, and still the systems defended will be compromised. In the current system, there is no compensation for this disparity in the investment required. The Internet has changed the economics of many things, none the least of which is security and privacy. That recent change, and many others, needs to be factored into our approach.

https://scholarship.law.nd.edu/jleg/vol43/iss1/5/

(3) More Management Incentives: Missing from the CSRC report is an examination of the decision-makers and why they make the decisions they do. Why is management not allocating sufficient funds to provide adequate information security and privacy? The answer is they are incentivized to cut-corners, to keep costs down, to increase profits, etc., and all that often compromises information security and privacy. The incentive systems that management now uses must be reengineered if we are going to have managers making the right decisions that bring about an adequate level of information security and privacy. This is especially problematic because secure information systems infrastructure is a long-term investment, and the incentive systems that exist now are short-term in their focus. See the article entitled (and link): "Solving the Information Security & Privacy Crisis by Expanding the Scope of Top Management Personal Liability," by Wood (December 2016, Journal of Legislation).

/s/ Charles

Charles Cresson Wood, Esq., JD, MBA, MSE, CISSP, CISM, CISA, CGEIT Independent Information Security & Privacy Consultant http://www.infosecurityinfrastructure.com