The following information is in response to the RFI for Developing a Framework to Improve Critical Infrastructure Cybersecurity

Security is an issue with a strong commons background mixed with externalities. By commons background, I am referring to the age-old dilemma of who manages the common area where all can deplete a common area with no one responsible for the common area. Economic externalities are costs which results from an activity or transaction and which affects another party who did not choose to incur that cost or benefit. It is recognized in economics that for goods with externalities, unregulated market prices do not necessarily reflect the full costs of the transaction.

In security, especially with critical infrastructure elements, both of these elements play a role. Using electricity as an example, as customers, we all share in the same pooled resource of electric delivery. Each of us desires complete use of the maximum amount of the resource while only paying "for the portion that we use" or variable cost of our electrons. Issues such as cyber security, are something we want the other party to pay for. From the utilities' perspective, the cost of an outage, for whatever reason, is limited to the revenue they did not collect from loss of sales. The cost to the customers of not having power is an externality that is not figured into the cost in a typical ROI equation. In the case of electrical utilities, this is dealt with through regulation, but how does this concept span across all critical infrastructures?

Regulation is the only known solution to externalities and commons issues, but regulation with respect to cyber-security issues and critical infrastructure is a hotly debated topic. One of the regulation issues revolves around who does the regulation. In the electric power sector, this is done through a series of regulatory entities that cover different aspects of the complete utility value chain from generation to distribution to customer. The net result is a series of differing and overlapping responsibilities with respect to cyber security issues. In the end, regulation becomes a compliance issue, that many argue is neither agile enough or connected to the business in a manner that best resolves the issues.

I think it can be argued that regulation will be a necessity to have viable cybersecurity capability and functionality in critical infrastructure environments. The form of said regulation is the challenge. In the case of the electric industry, the NERC CIP series is viewed by many as slow, less than completely effective and costly. Adopting this consensus based model across multiple infrastructures will only add cost ad bureaucracy, and do little to manage the risk associated with cybersecurity. When regulatory changes take years to percolate through a system, and the antagonist of the changes is an agent that changes in a timescale of weeks and months, then the responsiveness mismatch produces ineffective solutions. And when regulation creates a "floor" for performance, and other regulatory bodies in pursuit of cost effectiveness make the floor also the ceiling, then the result is one where people do what compliance dictates, not in the original interest of the regulation, but to be found not in a non-compliance or finable state.

There are other regulatory approaches that have been used in various industries. In the nuclear power industry, there is a standard that is applied to radiation exposure: ALARA – As low as reasonably achievable. As defined in Title 10, Section 20.1003, of the Code of Federal Regulations (10 CFR 20.1003), ALARA is an acronym for "as low as (is) reasonably achievable," which means making every reasonable effort to maintain exposures to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, the economics of improvements in relation to state of technology, the economics of improvements in relation to benefits to the public health and safety, and other societal and

socioeconomic considerations, and in relation to utilization of nuclear energy and licensed materials in the public interest. Although some may say this adds to cost, when one views the total costs associated with radiation exposure, this methodology results in the lowest overall total cost.

Lawyers represent another approach to regulation. Rather than having the government or other body regulate lawyers activities and behavior, they operate a form of self-regulation through a professional society known as the bar. This removes the problems associated with a third party who does not have any direct involvement in the outcome of a situation, providing a safeguard against solutions with unintended consequences. One can argue that many of the complaints towards government regulation come from unintended consequences associated with a third party regulation.

For critical infrastructure, some combination of these two elements can provide the best solutions. The government, acting in the interest of society (we are focusing on critical infrastructure) sets high level standards such as ALARA. In fact, a direct corollary, in which all cyber security risk is identified and minimized to as low as practically possible, consistent with the purpose of the critical infrastructure being served, taking into account the state of technology, the economics of improvements in relation to state of technology, the economics of improvements in relation to benefits to the public and safety, and other societal and socioeconomic considerations, and in relation to utilization of the critical infrastructure in the public interest. Then, enable professional groups, acting like the bar, to determine appropriate methods of how to achieve these objectives. A key element is the inclusion of the total security costs, not allowing cyber security to be cast off as an externality for another party to pay. In the end, the risk remains and if it is transferred as an externality, it only makes it a cost that cannot be efficiently dealt with by the third party.

Wm. Arthur Conklin, PhD
CISSP, CSSLP, CSDP, CRISC, Security+, CASP, IAM, IEM, DFCP
Associate Professor, Department of Information & Logistics Technology
Director, Center for Information Security Research and Education
College of Technology
University of Houston
312 Technology Building
Houston, TX 77204
(713) 743-1556 (o)
(210) 379-3671 (c)
(713) 743-4032 (f)

A Carnegie-designated Tier One public research university

http://tech.uh.edu/faculty/conklin