Additional Suggestions for a Cybersecurity Framework to Improve Critical Infrastructure Cybersecurity

James A. Lewis, April 2022

NIST has an opportunity to build on the global success of its 2014 Cybersecurity Framework mandated by Executive Order 13636. To help do this, NIST can take into the account the policy problems that that helped shape the original Framework. One reason for the development of the 2014 Framework, was the failure of Congress to pass comprehensive cybersecurity legislation that would have imposed mandatory requirements on companies. The Obama Administration adopted an approach where sector specific regulatory agencies used their existing authorities to mandate (as far as possible) that the companies they regulated adhered to a standard of best practices. The 2014 Framework laid out many of these best practices.

The 2014 NIST Framework should be updated to reflect changes in how technology is used and supplied (such as the growing adoption of a third-party service model). It should focus on the organization and protection of sensitive data, identify coding requirements, build resilience in services, and lay out steps to harden and secure internet-connected devices. It can draw on lessons derived from the SolarWinds incident and others on the frequent neglect to observe basic cybersecurity practices in both coding and operations. It offers the opportunity to define what "good" means for cybersecurity (e.g., the goals companies should pursue) and promote the observation of basic best practices, which are well known if not always observed.

In retrospect, the 2012 legislative failure was probably the best outcome at that time. The Department of Homeland Security (DHS), the intended regulatory agency, was not ready for this mission, nor did useful standards exist to identify what actions should be mandated to improve cybersecurity. The NIST Framework and other work undertaken in the decade after 2012 help remedy this and offer an opportunity build on what has been developed after 2012. Key among these is the development of a sector specific, limited regulatory approach based on the NIST Framework identified in the 2013 Executive Order (EO) 13636. The sector-specific approach remains best, given the size and complexity of the American economy. Sectoral agencies will have the necessary knowledge of their "customer base" for effective oversight and collaborative work. Appointing a single agency to be some kind of uber-regulator (the legislative proposal in 2012) would be both politically difficult to achieve and most likely ineffective. NIST should as much as possible draft language that is applicable to all sectors rather than take a sector-by-sector approach.

To guide its thinking on the requirements of a revised Framework, NIST may wish to consider an expanded approach to mandatory requirements. While the Framework itself would not impose such mandatory requirements, it should be drafted in such a way to permit this if the current Administration or some future Administration decided to take this path. In essence, a new approach would begin with an updated NIST Framework to which entities would self-certify that they observed in their practices. Self-certification can be sufficient to ensure conformity with the Framework and avoid the complexity and expense of certification regimes. To work, self-certification would be reinforced by incident notification requirements in the event of a success hack. Notification of a successful hack could trigger some kind of review (perhaps by DHS's new Cyber Review Board) on the degree to which the NIST Framework had been observed.

Some have suggested that this kind of approach could, when negligence was found, draw upon precedents from consent decree mechanisms (similar to those used at the Federal Trade Commission or the Department of Justice) to provide an increased degree of accountability. However, any application of the Framework should be limited to a select number of facilities proving critical services. A new mandatory approach could be limited to critical infrastructure at greatest risk (building on Section 9 of EO 13636 or some of the proposals in pending legislation. Accountability and scope are matters for policy and law, but the intent of a new Framework effort should be to provide the technical and intellectual underpinnings of improved cybersecurity.

As before, the Framework should be as short as possible and not encyclopedic. The target audience for the Framework is the C-Suite and the Board of Directors, not the technical or engineering community, and it should be drafted appropriately. It should lay out specific requirements and objectives with as much specificity as possible. NIST and other elements of the executive branch charged with cybersecurity can begin work on this Framework with a vision of what is essential and mandatory, to be adjusted or expanded based on comments received.

This approach or some variant of it builds on the work NIST begun in 2014. It would build not only on the EO 13636 and the 2104 Framework, but on the tremendous progress in other Federal initiatives, such as in Software Bill of Material (SBOM) effort and the requirements for the development of secure software and services found in the 2021 EO 14208. SBOM and EO 14208 mandates, with their emphasis on best practices, security coding, and software provenance, will address most supply chain issues. While sector specific agencies could retain responsible for implementation under their existing legislative authorities, the new National Cyber Directorate could direct overall coordination.

This new effort should not be seen as final but as another step to a more secure cyberspace. Striking the right balance between mandatory requirements and incentives for voluntary actions to improve cybersecurity must take into account sector and company needs, but there is a growing consensus that it is time for mandatory requirements. A review of earlier technologies from the steam engine to the airplane suggests that it take between 25-40 years to develop adequate regulation to protect public safety. The internet was commercialized only 26 years ago, so we remain at an early stage, but it would be preferable to to wait another 14 years to develop effective parameters for security