Bond Case Briefs

Municipal Finance Law Since 1971

The National Cybersecurity Strategy: A Guide for Critical Infrastructure Owners and Operators

Protecting critical infrastructure has become a national security priority. On March 2, 2023, the Biden administration released the National Cybersecurity Strategy, a far-reaching document that sets forth its vision for the nation's public and private cyberdefenses.

The initiative seeks to shift some of the burden of mitigating cybersecurity risks away from end users and critical infrastructure operators to the private sector enterprises that are best-positioned to make meaningful advancements in security and resiliency. The Strategy also emphasizes realigning incentives to favor long-term investments for the private sector.

The Strategy is organized around five pillars:

1. Defend critical infrastructure.
2. Disrupt and dismantle threat actors.
3. Shape market forces to drive security and resilience.
4. Invest in a resilient future.
5. Forge international partnerships to pursue shared goals.

Each pillar contains specific strategic objectives designed to build on prior programs and guide the implementation efforts of governmental and private sector entities.

The New Regulatory Wave

The Strategy seeks to usher in a new cybersecurity regulatory paradigm for critical infrastructure sectors by departing from voluntary guidelines to mandatory cyber regulations, which the Strategy concedes will require some legislative action. Driving this initiative is a demand for a "more intentional, more coordinated, and more well-resourced approach to cyber defense."

The Strategy also recognizes the heightened risks in the current era of global digitalization and deepening digital dependencies accelerated by emerging technologies. Rapid technological advancements are also forcing critical infrastructure sectors to grapple with the risks of converging informational technology and operational technology systems, which must be designed and secured in very different ways. A complicated geopolitical environment exacerbates those risks, as state-sponsored cyberthreats to critical infrastructure are on the rise.

While specifics of how the Strategy will be carried out are uncertain, implementing the objectives promptly will be key in an evolving world, where threats may outpace regulation and lawmaking. The Biden administration has alluded to some overarching principles in addition to mandatory regulations, such as security by design as a core business principle, operational availability to avoid systemic interruptions, and the promotion of rulemaking harmony across jurisdictions.

The New Insurance

Cyber insurance is now offered as a standalone type of coverage that earns billions of dollars in premiums for the insurance industry. This relatively "new" type of insurance covers various types of liabilities or direct losses from events related to electronic activities and systems. Part of the Strategy involves exploring a federal cyber insurance backstop, reflecting a partnership between the government and insurance industry to support the issuance of cyber coverage for commercial entities, consistent with national goals. The benefits of a cyber insurance backstop could be multifold:

- **Benefits to Insurers:** Increased financial certainty and stability, and a potential mechanism for more standardization and data sharing.
- **Benefits to Insured Companies:** Potentially more affordable coverage, as well as potential standardization and improvement of terms.
- **Benefits to the Public:** Increased prevalence of cyber insurance, encouraging a more sophisticated, resilient society, with the potential for improved data sharing among public and private actors.

Challenges

For all of its benefits and forward-looking initiatives, there are some challenges with analyzing and implementing the Strategy. The first is harmonization of duplicative or overlapping requirements. Companies facing a cyber incident are often challenged with juggling multiple (sometimes conflicting) reporting requirements, which can divert personnel and resources away from remediating the actual threat. The Strategy recognizes the challenge of regulatory harmonization, but is scarce on implementation details.

One of the trickiest pieces for companies to navigate is understanding how the agencies may address the recommendations from the Strategy with the tools they have today—not just their processes and people, but also the extent of their legal authority. Some federal agencies already have significant and broad security and safety authority in the critical infrastructure sector, and the Strategy makes it clear that regulators should consider leveraging those powers to start executing outlined priorities.

Recent Federal Initiatives Targeting the US Cyber Posture

In addition to announcing the Strategy, the federal government has taken steps in other areas, while coordinating with state municipal authorities, private sector, and federal stakeholders to improve the national cyber posture and capabilities in the face of intensifying cybersecurity threats.

Among these efforts include guidance by the Cybersecurity & Infrastructure Security Agency (part of the US Department of Homeland Security) on software bill of materials and updating the cross-sector Cybersecurity Performance Goals; the proposed requirements by the US Securities & Exchange Commission for cybersecurity risks; the US Environmental Protection Agency's memorandum for public water systems; and the expansion of the Transportation Security Administration's pipeline-focused security directives to the aviation and rail sectors.

Assess. Plan. Monitor.

For critical infrastructure owners and operators, there are several key steps to take today:

- **Policy Advocacy**: Regulator education is critical. Consider participation in stakeholder opportunities to shape requirements before formal rulemaking, if possible.
- **Interdisciplinary:** Compliance can be achieved through coordination among IT/OT, security,

compliance, and legal departments, as well as by supply chain management, human resources, finance, and other personnel. Shortchanging one area may increase a company's risk exposure.
- **Cultural Change:** Ensure that cybersecurity is taken seriously not only at the highest levels, but also throughout the entire organization. Use guidance, standards, best practices, and continuous training to shore up cyber posture.

Morgan, Lewis & Bockius LLP – Arjun Prasad Ramadevanahalli, Stephen M. Spina and Robert Jacques

June 23 2023