Published on *The National Law Review* https://natlawreview.com

Leveraging “Public-Private Collaboration” for Critical Infrastructure Cybersecurity

Article By:

Kurt R. Erskine

Romaine C. Marshall

In March, the White House issued its long-awaited National Cybersecurity Strategy. The strategy includes five pillars, Pillar One being “Defend Critical Instructure” with its first and second subparts focusing on (1) establishing cybersecurity requirements, and (2) scaling public-private collaboration.[1]

The Strategy states that collaboration between the public and private sectors is essential, and that participation in “public programs” to improve security and resilience should be rewarded, resilience being the ability “to withstand and recover rapidly from disruptions, deliberate attacks, accidents, and naturally-occurring threats or incidents.”[2]

Easier said than done. Two weeks ago, a bipartisan committee for developing a strategic approach on cyberspace issued Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure. The summary begins by stating: “Few things more directly impact Americans’ security and well-being than the reliability, availability, and safety of critical infrastructure.”

True to the report’s title, the summary then identified flaws, particularly with the design and implementation of public-private collaboration, including:

- The implementation of policies — and the organization, funding, and focus of the federal agencies that execute them — is inadequate.
- An incremental approach is not working, especially as both physical and — especially — cyber threats to critical infrastructure continue to escalate.
- Processes for sharing information, responding to emergencies, designating priorities within sectors, and promoting resilience are insufficient.

If the Commission’s report casts a pall, it’s for good reason. In the last two months the FBI, the Critical Infrastructure Security Agency, and others have issued detailed advisories about destructive attack vectors with names like Snake, Volt Typhoon, CosmicEnergy, and victims like MOVEit whose

downstream victims number in the thousands and include government agencies.3

The public sector advisories are notable – instead of only providing mere tips and pointers on how to update such things as access, patch, or vendor management programs, the advisories describe in detail the TTPs (tactics, techniques, and procedures) being utilized by global threat actors, and how to identify, prepare, and respond.4

In addition, reports by private sector organizations like Microsoft and Mandiant have described how nation-state actors supported by their governments are targeting a variety of sectors including education, small businesses, and media organizations, and critical infrastructure sectors such as government facilities, financial services, and communications.5

Considering the intensifying threat landscape, private sector organizations should consider seizing an opportunity to emphasize their public-private collaboration and limit potential legal exposure (i.e., be "rewarded") by updating their cybersecurity incident response plans, risk assessments, and security programs, to include the following:

Incident Response Plans

- Incorporate contact information for law enforcement and regulators (FBI, CISA, and DHS) in your incident response plan roster. A website for reporting incidents 6 and a Cyber Resource Hub 7 are just some of the resources made available by the regional Department of Homeland Security offices.

- Include draft letters and documents that demonstrate the types of cyber event information required (e.g., CISA's "10 Key Elements to Share").8

- Compare your incident response plans with public sector guidance 9 and consider using CISA's Tabletop Exercise Packages to test your plan.10

Risk Assessments

- Consider CISA's six-step process for conducting risk assessments.11

- Use 'free' government agency tools for preliminary, self-risk assessments to determine maturity and alignment levels.12

- Ensure that any external reporting obligations are assessed with internal incident reporting capabilities (e.g., 24/72-hour reporting windows).13

Written Information Security Programs

- Ensure programs align with the cross-sector Cybersecurity Performance Goals(CPGs) developed by CISA to help organizations prioritize and reduce risk.14

- Consider referring to various US States' safe harbor statutes that encourage mapping programs to established frameworks such as NIST special publications like the Utah

Cybersecurity Affirmative Defense Act.15

- Understand that programs must be adjusted in light of any changes … that an organization knows or has reason to know may have an impact on effectiveness.

National Law Review, Volume XIII, Number 175