NATIONAL SECURITY FOCUS ON CYBERSECURITY FOR CRITICAL INFRASTRUCTURE SHARPENS

Decemember 1, 2022

Last year Colonial Pipeline halted one of the United States' largest pipeline systems due to a ransomware attack.[1] Within days a state of emergency was declared in 17 states. A few days later the pipeline resumed service, and Colonial acknowledged it paid $4.4 million to cyber criminals.[2] For critical infrastructure, Colonial Pipeline was a turning point.

Executive Order on Improving the Nation's Cybersecurity Sets Tone

On May 12, 2021, in response to Colonial Pipeline and other cybersecurity incidents, President Biden issued the "Executive Order on Improving the Nation's Cybersecurity," an 18-page order with numerous deadlines for specific action items to be completed within days, weeks, and months, and several strong objectives:

> The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems …. and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

To achieve these, the Executive Order eschewed "incremental improvements," mandated "bold changes and significant investments," and directed the government to "partner with the private sector." For many in cybersecurity, a public and private sector partnership is new territory. Nevertheless, guidance has been issued and legal obligations are being established.

White House Issues Fact Sheet and National Security Memorandum

On July 28, 2021, the White House released a Fact Sheet to address "growing, persistent, and sophisticated cyber threats" through new approaches with "critical infrastructure owners and operators." In addition to Colonial Pipeline, the White House referred to JBS Foods, the meat processor that paid an $11 million ransom in June 2021.[3]

On the same day, President Biden signed a National Security Memorandum, "Improving Cybersecurity for Critical Infrastructure Control Systems" (NSM) directing

Authors

Jose A. Abarca
Shareholder
jabarca@polsinelli.com

Romaine C. Marshall
Shareholder
rmarshall@polsinelli.com

1 https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

2 On June 7, 2021, the Department of Justice announced the recover of $2.3 million in cryptocurrency that was paid to the cyber criminals (https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside).

3 https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/

the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) and other agencies to develop cybersecurity standards for essential services like "power, water, and transportation."

CISA's objectives are to "lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure." To accomplish these, CISA and its employees (currently 2500) have been working across public and private sectors with partners to build a more secure and resilient infrastructure for the future since 2018. [4]

According to CISA, there are 16 sectors (shown below) whose assets, systems, and networks, whether physical or virtual, are considered so critical to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. [5]

Since the issuance of the Executive Order, Fact Sheet, and NSM, a vast patchwork of proposed laws, regulations, and industry standards have emerged within some critical infrastructure sectors. In the Energy Sector, for example, electric utilities have released 17 cybersecurity considerations for industrial control systems and operational technologies.[6]

Overall, for the "public and private sector partnership" to be effective, a greater understanding of the threat actors and their tactics, techniques and practices is required. Awareness has grown as overwhelming evidence has pointed to threat actors acting within and/or with permission from Russia,[7] China,[8] North Korea,[9] and Iran.[10]

---

4 https://www.cisa.gov/strategy, and https://www.cisa.gov/critical-infrastructure-sector-partnerships.

5 Presidential Policy Directive 211 identifies 16 critical infrastructure sectors: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

6 https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies

7 https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/ , and "Act Now" Fact Sheet (March 21, 2022).

8 According to Microsoft, China stepped up its espionage and information-stealing cyber attacks in order to counter the USA's attempts to increase its influence in Southeast Asia (https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022).

9 https://www.cisa.gov/news/2022/07/06/cisa-fbi-and-treasury-release-advisory-north-korean-state-sponsored-cyber-actors

10 https://www.cisa.gov/uscert/ncas/alerts/aa22-320a (Iranian Government-Sponsored APT Actors compromise Federal Network, etc.).

National Security Focus on Cybersecurity for Critical Infrastructure Sharpens

Recent Fact Sheets Show Some Progress, But Clarity is Needed

In March, the White House urged organizations to ensure steps were taken in response to "evolving intelligence that Russia may be exploring options for potential cyberattacks." In the short term, these steps included technical requirements such as multi-factor authentication. In the long term, building security into products – "bake it in, don't bolt it in."[11]

Then in October and November, the White House highlighted aspects of its approach to "lock our digital doors," and CISA's partnership with the Chemical Sector including an action plan focusing on facility risk assessments, and the formation of numerous programs designed to develop a "robust and skilled workforce" to protect national interests. [12]

In addition to these announcements, numerous government agencies and related organizations have issued new reports and proposed new laws, regulations, and industry standards, greatly expanding the tapestry of an already expansive patchwork. It's chaotic, befitting the complexity of the underlying networks, systems, and infrastructure.

For example, a few weeks ago a government report found that more than 1,600 offshore oil and gas facilities are so vulnerable that a cyberattack could resemble the 2010 *Deepwater Horizon* disaster.[13] Railway infrastructure has been experiencing cyberattacks overseas, while in the U.S. even a railway labor strike could inflict economic damage reaching $2 billion a day.[14]

But, to tie together cybersecurity obligations for all critical infrastructure sectors, CISA has released preliminary Cross-Sector Cybersecurity Performance Goals (CPGs).[15] The CPGs are intended to be:

- A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
- A combination of recommended practices for IT and OT owners, including a prioritized set of security practices.
- Unique from other control frameworks as they consider not only the practices that address risk to individual entities, but also the aggregate risk to the nation.

The CPGs are layered. They are also indicative of how far the federal government is willing to go to "partner with the private sector" in the interest of national security. At a minimum, the CPGs provide covered entities with tools and resources to enhance their cybersecurity programs.

In the weeks and months that follow, CISA's role will expand to harmonize numerous cybersecurity measures across sectors. For covered entities, the best approach of all will be the proactive one espoused by cybersecurity and technology specialist, Ian Bramson:

> Put simply, you can regulate your way to compliance, but you cannot regulate your way to security. Regulations, by their nature, enforce a minimum standard across a broad range of companies. They are also focused on if you do something, rather than *how well* you do something.[16]

From a legal and compliance perspective, the last eighteen months since Colonial Pipeline have provided ample evidence of the cybersecurity risks organizations face. Setting aside for a moment the legal obligations, national security obligations provide an additional basis that is just as compelling.

---

11 https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

12 https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/,

13 https://www.gao.gov/products/gao-23-105789

14 https://www.nytimes.com/2022/09/14/business/freight-rail-strike-supply-chain

15 https://www.cisa.gov/cpg

16 https://www-cpomagazine-com.cdn.ampproject.org/c/s/www.cpomagazine.com/cyber-security/how-we-will-win-the-cyber-physical-battle-for-ot-security/amp/