ICIT - Institute for Critical Infrastructure Technology

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit (status pending), non-partisan group of the world's most innovative experts and companies that provide technologies and solutions to support and protect our nation's critical infrastructures.

Together, industry and government can solve the critical challenges facing the critical infrastructure community and determine how to maximize resources, leverage expertise, best use technology, and strategically align resources to support common missions and goals.

As an organization comprised of fellows from all political backgrounds, ICIT is uniquely well positioned to offer niche advisory to the policy community in the fields of critical infrastructure technology and cyber security.

Issue Analysis

HR 3696 National Cybersecurity and Critical Infrastructure Protection Act of 2014:

ICIT would recommend re-introducing this bill. There appears to be good synergy with the content and the direction of the Administration regarding information sharing. Further, it speaks to existing systems while also noting required additional structures to address the information sharing challenge.

Recommendations include the following:

- The definition of "Critical Infrastructure Sectors" should include universities, colleges as well as private research entities focusing on areas of concern critical to technology and cybersecurity development. This is in addition to traditional aspects such as medical, defense technologies, and advanced communications research.
- Title 1, Sec 227 (a)(1)(D) States that the Secretary will provide assistance "to reduce vulnerabilities." There does not appear to be any specific language for the mandating of Vulnerability Assessment and/or Penetration testing for those entities identified as Critical Infrastructure Sectors. This should be requisite, or at the very least include a provision requiring these services to be available upon request.
- It would be helpful to include a provision requiring the inclusion of private entities considered under the Critical Infrastructure Sectors in regularly (quarterly, biannual…etc.) held Cybersecurity event/response exercises. These should include all entities of concern for different types of cyber events: Cyberterrorism, hacktivist attacks, hack for profit (PII, PCI, financial breaches).

Information Sharing:

- Many federal agencies and private corporations, both large and small, have some form of cyber monitoring or risk analysis presently ongoing for their organizations. The point of clarification for many is defining what information to review that could create that "critical incident." In review of both the Target and Home Depot attacks as well many of the breaches that made headlines in 2014, we feel that it was not lack of information that was problematic, but rather sharing of important pieces of information to provide truly actionable context. Many organizations are overwhelmed with information from their present monitoring activities.

- Furthermore, the Treasury OCC in a recent RFI for Security Operations Center support noted the average log size is 1.5 billion events per day. This is a relatively small agency in comparison to our larger agencies and companies in critical infrastructure, such as DoD. Thus, the key question is how do we narrow this down so we are sharing information that is important. Failure to do so will ensure Target or Home Depot will likely continue to "miss critical incidents." Companies and agencies need the right information with a proper context and everything cannot possibly be digested, reviewed and handled on a daily basis.

Relationship between DHS and Industry:

- We are at the juncture where DHS has the opportunity to be recognized as a thought leader and trusted advisor to the private sector in the realm of Cybersecurity, and no longer considered to be "Big Brother."
    - This can only be achieved through successful partnering with private entities at all phases of developing policies and standards. Transparency with trusted entities within the Critical Infrastructure Sectors.
    - The DHS has quality programs such as the Software and Supply Chain Assurance program, which has demonstrated success in its outreach to industry, academia, and government.

Government/Infrastructure Provider Relationship:

Recent testimony by NIST and DHS on this topic covered the issues well. We agree with their position that leveraging NIST's CSF and threat intel sharing are the correct steps to protecting the U.S. against cyber threats. Threat sharing is important because it provides the defenders with near-real time actionable intelligence of attacks.

However, there are always privacy and liability concerns with sharing information with other. Those concerns are heightened when sharing with the government. Additionally, companies that have, or are sharing information with the government, often discover that while the government welcomes the information, there is little to no quid pro quo.

In other words, other than patriotic duty, there is little tangible gain for sharing information. Further, any cyber intelligence-sharing model must be bidirectional. With all of these concerns, a possible way ahead is instead of the government (DHS or the IC) being responsible for managing all the shared data, a third party (i.e., non-profit entity or an FFRDC) may be a more efficient option.

We should also be placing protections around the names of the companies that share specific information with the U.S. government. The trusted insider that harvests data to share publically (e.g., Snowden) irrevocably harms U.S. companies to compete in the international marketplace.

In addition, each vendor CEO should be approached about who are his or her two most trusted individuals. One should be a technology person, such as the lead engineer; the other should be a businessperson, such as the CFO. These two people should receive clearances and be provided a secure platform for collaborating with government about threats and weaknesses.

Anonymous identities should be used in a secure platform to encourage collaboration with other companies that may be business competitors. For example, Bank Of America (BoA) may not want to share cyber threat intelligence with Wells Fargo. However, if each person in the secure platform had an anonymous username they could more likely be motivated to freely share information without concern for the competition. Thus, at the end of the day BoA and Wells Fargo would benefit because they would be working with government to help each other be better protected.

Next Generation of Cyber Workforce:

- Agencies tasked with protecting critical infrastructure need to partner with Universities to provide advanced levels of cybersecurity training for those programs generating the next generation of cybersecurity professionals.
- Make cybersecurity a more robust part of every curricula dealing with information systems and their touch points.
    - Reinforce the commitment to cybersecurity education through additional grant funding, scholarship programs for those areas of focus.
- Public awareness campaigns to reinforce the need for better information security starting at home.
    - We need to create a “Culture of Security” at home and in the workplace, no differently than OSHA has created a culture of safety.
- The US Air Force has developed an innovative program entitled “Cyber Patriot”
    - This program is designed to get high school students involved with Cybersecurity, and encourage support for programs such as LaunchCode, a 5-month boot camp training for the unemployed in St. Louis. It provides basic programming training and is aimed at prospective apprentices. Similar programs for cybersecurity that train workers on the basics of cybersecurity and development of apprentice

programs to help fill the gap in cybersecurity professionals would be welcomed.

**Expert research contributed by the following ICIT Fellows*:

- Danyetta Fleming Magana (ICIT Fellow - President and Founder, Covenant Security Solutions)
- Shelley Frazier (ICIT Fellow - Chief Operating Officer, Covenant Security Solutions)
- William J. Billings (ICIT Fellow - Security Strategist, U.S. Public Sector, HP)
- Cynthia Cullen (ICIT Fellow - Security Strategist, Northeast, HP)
- Stan Wisseman (ICIT Fellow - Security Strategist, Southeast, HP)
- Ryan Kalember (ICIT Fellow - Chief Product Officer, WatchDox)
- Dan Skinner (ICIT Fellow - Federal Partner & Solutions Architect, WatchDox)
- Dan Waddell (ICIT Fellow - Director, Government Affairs, (ISC)2)
- Chris Schumacher (ICIT Fellow - Sr. Technology Consultant, New Light Technologies)
- Parham Eftekhari (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Morgan P. Muchnick (Senior Director of Legislative Affairs – Institute for Critical Infrastructure Technology)