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 key 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. According to Mr. Dan Waddell (ICIT Fellow and Director of Government Affairs at (ISC)2) "DHS and industry are doing many things right…DHS should resist the temptation to reinvent the wheel. Rather, it should focus on what works and make it better."

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, cyber security and rural health technology.

Cybersecurity and Information Sharing

Recent legislative activity involving information sharing has, among other things, included the possibility of creating a DHS-controlled information-sharing portal. ICIT Fellows believe that if a portal is created, the following principles should be taken into consideration:

- Reporting of events should remain optional, unless the event has affected an organization that has been categorized as part of the United States' critical infrastructure.
- Organizations, Educational programs, facilities determined to be of critical national security importance should not have the ability to opt out of a rigorously implemented and monitored cybersecurity program.
- A successful partnership between the government and private sector organizations must revolve around a common operating picture that includes education and training for private sector cybersecurity professionals, and inclusion/protection of private sector entities in Critical Infrastructure sectors (Research/Academic institutions, Medical Research, defense technology firms…etc.).

Further, the specific company identity should be kept confidential in most cases.

- Companies with a legal responsibility to report breaches due to concern over PII, PCI or financial breaches, and other types of protected data losses will already do so to maintain compliance with legal mandates.
- Publicizing successful breaches fuels additional attempts for notoriety from Hacktivists, Hack-for-profit, and cyberterrorists.
- This also erodes the trust of the average citizen/consumer who does not typically understand the severity of a breach, or the steps taken to prevent and/or recover from a breach.

Trust among industry and private Internet users will be hard to create. Concerns include:

- After the Bradley Manning and Edward Snowden breaches, the level of confidence in the ability of governmental organizations to protect data from even an insider threat has been greatly diminished in both the public and private sectors.
- The average citizen has difficulty distinguishing between GovSec breaches and those that have taken place in the private sector over the course of the past few years (Target, Home Depot…etc). This tarnishes the reputation of Information/Cyber Security as a whole in the US with little distinction between the private and government sectors.

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

- Darryl E. Peek (ICIT Contributor - Federal Network Resilience Integrated Cybersecurity Services, IT Security Specialist, US Department of Homeland Security)
- Chris Schumacher (ICIT Fellow - Sr. Technology Consultant, New Light Technologies)
- Dan Waddell (ICIT Fellow - Director, Government Affairs, (ISC)2)
- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Parham Eftekhari (Senior Fellow – Institute for Critical Infrastructure Technology)
- Morgan P. Muchnick (Senior Director of Legislative Affairs – Institute for Critical Infrastructure Technology)