ISA Comments to Hathaway on creating an International Cyber Security Anchor Program

CREATING INTERNATIONAL CYBER SECURITY BY PARTNERING WITH INTERNATIONAL INDUSTRY

One of the biggest hindrances to the US government's approach to international cyber security is its preoccupation to crafting this policy primarily on a nation state to nation state basis.

While this traditional approach is intuitively logical, after all the US is a nation state with a robust international infrastructure, it is in conflict with the inherent nature of the internet.

The internet generally does not operate on or respect nation state boarders. Moreover, attempting to accommodate the numerous independent nation state interests adds additional complications to establishing a sustainable system of international cyber security.

The US might be able to move more quickly and effectively to establish international security standards and practices by working directly with the multi-national corporations based in or doing primary business in the US.

As data security is increasingly recognized as a problem area internationally the US could capitalize on the potential marketing advantages of providing security while boosting trusted business partners in the marketplace and cementing the USG's status as the leader of world-wide cyber security

US GOVERNMENT CAN CREATE A STRONG POSITIVE EFFECT THROUGH MODELING

It is axiomatic that the vast majority of the cyber infrastructure is owned, operated and controlled by private industry.

As a result, it is industry's role to implement the security procedures needed to establish broad scale cyber security. It is government's role to motivate industry to create and implement these standards and practices.

Obviously, the USG cannot abandon its work with nation states or groups of nation states. However, as a compliment to these efforts the USG can establish a model for working with industry by providing incentives for improved cyber security.

In previous ISA comments sets of standards and practices empirically proven to be effective in combating the vast majority of current cyber breaches have been identified.

The USG can initially create a model for government interaction with industry by rewarding entities that voluntarily comply with empirically proved effective standards and practices with market incentives.

Punitive approaches (fines/market restrictions , etc.) outside of a confined group of regulated industry sectors, will likely have the counterproductive effect of driving business to more friendly environments negatively effecting the US economy and simultaneously reducing the USG's ability to improve cyber security. In a converged world economy the ability of major industries to operate primarily off-shore while doing business in the US should not be underestimated

USG OUGHT TO LEVERAGE INTERNATIONAL BUSINESS BY DESIGNATING INTERNATIONAL "BUSINESS SECURITY ANCHORS"

Modern large businesses (including "US businesses") generally operate in multi-national level. The USG ought to leverage this international reach to promote international cyber security.

Creating a domestic market incentive program for businesses operating in the US will be a first step in creating an international program as multi-national businesses have inbred incentives to have their full systems, domestic and international, operate on similar standards and practices. Thus standards and practices adopted for US operations may well be adopted in international sites to create full system coherence.

A second, more affirmative step, would be for the USG to enlist via contract, US based, or other trusted organizations, as "Business Security Anchors"

The International Business Security Anchor program is modeled on the Cyber SAFETY Act enacted following 911 and the proposal Cyber Safety Act suggested in previous ISA comments.

The company designated as a "Security Anchor" would have the responsibility of not only following designated cyber security practices and procedures, but exporting these practices in off-shore locations where they operate.

Anchors would be expected to utilize and integrate the practices and standards subject to the domestic incentives as a condition of maintaining their status.

They would be charged with the responsibility to do translation services as required and recruit and conduct localized training and outreach within their regions.

Anchor status would be non-exclusive, meaning there could be multiple competitive anchors in a region.

The USG would provide and permit this entity to distribute security notices, practices, tools and training created and provided by the USG, much as USG currently does with domestic entities through US CERT and Sector Coordinating Councils. (Obviously this material would be non-classified)

The anchor organizations would have several market incentives for participating. They would be permitted to market themselves as designated security anchors (following a US certification

program as complying with the empirically proven practices modeled on the SAFETY Act procedure). They could be permitted to charge for the training and distribution of information and they would qualify for other US based incentives discussed in previously submitted comments in this effort.

By being the provider of the core cyber security data and practices used by the anchors the USG would establish and maintain leadership in this field.

The USG would also establish a relatively economical distribution system for the dissemination of needed cyber security information and training.

Finally, since the cost of developing and providing the data are already covered through domestic distribution of these same services, the cost to the USG would be minimal.

Since the incentives are US domestic in origin they essentially by pass the organizational difficulties of negotiating international agreements (the standards embraced for incentive could be internationally based e.g. ISO standards)