Cross cutting Issue #2 How Can we create public private partnerships that extend to action plans that work?

I. SOLVING THIS PROBLEM IS OF CRITICAL IMPORTANTCE

Of all the issues the 60-day review is considering, this one may be the most far reaching in its implications.

This is because due to the inherent characteristics of the Internet, and unlike many traditional infrastructures, it will be impossible for the US government to create a sustainable system of cyber security without the active, voluntary and continuous participation of the private sector.

II. WHAT IS, AND IS NOT, A PUBLIC PRIVATE PARTNERSHIP

To analyze this critical issue clarity of definition is necessary. Not all conferences, meetings or organizations or even joint projects which include both public and private sector participants are usefully understood to be "partnerships."

In a true partnership entities with at least roughly equivalent power over the relationship and at least somewhat differing goals and objectives agree to compromise their interests and jointly develop an action plan to achieve mutual gain for each other's objectives as well as mutual objectives.

So when a company that makes servers "partners" with a company that sells routers, they may jointly develop an action plan enhancing their own separate bottom lines. Should one company seek to dominate the goal state (e.g., "We really want to just sell servers") the partnership, even if successful in the short term, will be unsustainable because of the lack of trust that is generated by the dominance of one side's interests.

In the case of the public and private sector working together, it is the government's role to serve the broader public interest. Industry's legally mandated goal is generally to serve the shareholder's interest.

So when government asks for industry input on a new regulation, notwithstanding the collaborative effort, it cannot truly be considered a "partnership" since the government has power over the regulated entity to set the action plan in motion and the industry input is to primarily serve the government's (or the general public's) objectives.

Similarly, when industry voluntarily assists government In pursuit of a governmental objective, such as emergency services, not withstanding the cooperative effort and unquestionably worthy goal state, this is not a public private partnership, since industry's shareholder interests are not being served. Such a, laudable, effort might best be understood as a public service, not a true partnership. Because the action plans for these efforts are, appropriately, government directed and the goal states are to serve the public interest, not the private interest, they tend to be difficult to sustain beyond the emergency situation and especially difficult to sustain in times of general economic difficulty.

III. DEFINING ROLES AND RESPONSIBILITIES IN THE PUBLIC PRIVATE CYBER SECURITY PARTNERSHIP

Current public private partnerships in this space have at best unclear or ill-defined roles and responsibilities for the industry and government partners.

Certainly specifying roles and responsibilities can be difficult, especially if the purpose of the partnership itself is only broadly defined. However, failure to do so will almost certainly lead to confusion and inefficiency which can and must be avoided.

Virtually every business relationship, including those between government and private industry, does clearly specify the roles and responsibilities of the partners.

With respect to cyber security we propose that roles and responsibilities ought to be based on the following model.

Government Role

1. Secure government infrastructure
2. Serve as model for industry
3. Provide industry with information in a timely and actionable format
4. Assure private infrastructure operating under government provided agreements (e.g. public utilities) are secure within the bounds of public interest requirements
5. Provide incentives for companies operating in non-regulated environments to invest in security in the public interest beyond what the private entity will do to serve its own private interests
6. Provide research development and evaluation to cyber security technologies and practices for which there is not a private sector interest
7. Educate the public regarding cyber security hygiene

Industry Roles

1. Innovate develop and get to market technologies that will enhance a secure infrastructure
2. Develop standards and practices to address the continually evolving cyber threat
3. Share information with the government consistent with the public interest without violating their corporate fiduciary responsibilities
4. Work with the government to develop mechanisms to enhance overall cyber security
5. Implement good security technologies and practices consistent with their fiduciary responsibilities

V. PRINCIPLES NOT GENERALLY BEING FOLLOWED CURRENTLY FOR PUBLIC PRIVATE PARTNERSHIPS In THE CYEBR SECURITY SPACE

The premise of this question is that the public private partnerships currently being operated by government with the goal of enhancing cyber security can be, and must be, improved. It has been widely understood that while there are many efforts through which public and private entities speak to each other, rarely do these efforts yield action plans that can be shown to meet mutually beneficial objectives

Whatever the inadequacy of the current model it is not this author's view that the problem lies in lack of effort.

Rather, there are 5 central principles not generally followed which would enhance the state of partnerships for cyber security.

A. Pragmatism, not Ideology Must Rule

B. There Must be a Fuller Appreciation of Both Partner's Value Propositions

C. Action Plans Must be Jointly Developed

D. Existing Private Sector Mechanisms Ought to be More Fully Utilized

E. Evaluation Must be an Inherent Part of the Design of Partnerships

A. Pragmatism, not Ideology, Must Rule

Dating back at least to the National Strategy To Secure Cyber Space published by the Bush Administration in 2002, there has been a suggestion that we ought to rely on due market forces which will drive the private sector to make the investments needed to assure a secure cyber space. This view was fully consistent with the general market orientation of the Bush Administration

While obviously there has been a great deal of investment in information security over the past 7 years it is also obvious that the investments needed to fully and sustainably secure cyber space have not been made.

Recently there has been a countervailing view, suggested for example in the CSIS set of recommendations to the Obama Administration, that the US government must regulate (in some unspecified "right" way) to assure cyber security since the market has failed. This view might be considered consistent with a more activist government role generally attributable to a Democratic Administration.

However, these ideologically based policies fail to appreciate that the goal is not what is "right" but what will work.

The Internet is unlike any other infrastructure. It uniquely calls for a creative public private partnership drawing on the strengths of both market principles and government involvement.

The essential point is that as government seeks to design a partnership agreement with industry it needs to focus not on making the market work or punishing bad actors via regulation, but pragmatically assessing which sort of tools it has available and which are most likely to create a sustainable system of cyber security given the unique variables inherent to this infrastructure.

As argued above, regulatory interactions are not partnerships in the sense being discussed here. Regulation is appropriate to control corporate malfeasance, which is not the issue with lack of investment in cyber security, and as a trade-off for some broadly defined social contract, such as with the trade of utility regulation in return for exclusive franchises, which is also not the case with respect to cyber security. More importantly, such modalities are unlikely to work outside of limited arenas already characterized by strict regulation and confined economic domains.

For public private partnerships geared to address Internet security to work they must:

1. Have clear, reasonable and measurable objectives

2. Have identifiable resources adequate to the task the partnership is designed for

3. Be cooperative in nature, lacking punitive overtones characterized by regulatory models, so that trust and affirmative proactive steps are taken by both partners.

4. Have a recognized joint leadership structure in which both partners believe they have equivalent investment in and control over the workings of the partnership

5. Create action plans jointly, starting with a blank page in which both partners develop the goals and objectives of the partnership project to be undertaken

   These pragmatic principles have often not been present in existing public private partnerships. Too often organizations have been set up without clear missions, beyond "coordination" and then projects are retrofitted into the existing structures.

   Resources in such partnerships have often been functionally controlled by the government and been inadequate or conditional on meeting government specified (sometimes unspecified) criteria leading to functional control of the government partner over the program thus undermining the partnership and private sector commitment.

   Often action plans, when they do exist are created by government staff and contractors operating outside the partnership environment and then presented for the equivalent of regulatory style "notice and comment" to private sector "stakeholders," often without adequate time for true participation by more than a superficial level of private sector input leaving the private sector believing government is simply "checking the box" of private sector involvement

B. Fully Appreciate the Value Proposition

   The value of cyber security for the government is the common defense. While individuals and companies benefit from a strong national defense, the national interest is not, and ought not be, the value proposition for private interests..

   For the private sector the value proposition for investments in cyber security are what is justified by their individualized business plans.

   In order for the government to engage in maximally profitable partnerships with the private sector it is critical for government to alter their sector by sector

approach to one in which they appreciate the value proposition for industry on the level the industry partners' deal with these issues---the business plan level.

The market approach embodied in the National Strategy worked only to a degree because the multitude of individual entities that make up the abstraction called the "private sector" make investments not on a private sector basis, or even a sector basis, but on a business plan basis.

Companies can and do make investments in cyber security consistent with their perceived private interest. Over the past several years' substantial investments have been made to enhance these individual organizational security needs the market has indeed worked.

However, it is the public sector's responsibility to assure the "common defense" which would include the areas of security that are not justified by individual corporate investments. In fulfilling this public responsibility the government has a number of tools available to it including regulatory as well as market enhancement mechanisms.

If the government wishes to develop partnerships with the private sector they must create a value for the targeted entities that they, not the government appreciate.

Current public private partnerships are virtually never structured at this level.

This does not mean that the government must analyze the individual business plans of each entity, but rather that they must hold out business sensitive, not simply public interest benefits.

C. Action Plans Must be Jointly Developed.

Even though industry has the greater resources and responsibility to addressing cyber security, government still sees itself as the "senior partner" in its relationship.

This means that to often when current public private partnerships engage in projects they are typically initiated by the government partners to address government, interests. As good partners industry will attempt to assist government in these projects, but the effectiveness of the projects is sometimes compromised from the start due to government's "senior partner" role.

A corollary is that action plans, to the extent they are developed, are often drawn up by the government partners and then provided to industry ostensibly for comment, but only after the government partners have already become committed to them (and very often on unreasonably short time frames, especially compared to the time government takes in drawing up the initial "drafts" which communicates a lack of sincerity as to government's interest in industry input).

Thus projects begin on paths toward goals that are not developed in partnership, which leads to unenthusiastic commitment on the private sectors side, wasted time and effort, and products that are not as useful as they ought to be

(The current exercise in which Ms Hathaway seems to be reaching out for input to the private sector prior to developing a plan of action maybe a refreshing and encouraging departure from the typical process)

For example, and consistent with point 2, above, one of the first and highest priorities of the sector coordinating councils (SCCs), at the government's behest, was to assist in developing a sector based risk assessment.

Sectors are not attacked, companies are.

Government has decided to organize its approach to security based on supposed economic sectors. Given this approach it is perhaps logical that it would want a risk assessment of these sectors. However, industry does not organize its strategies or spending priorities on a sector basis. Thus producing a sector wide risk assessment, while convenient government analysis is of virtually not real world value to the companies within the sectors, each of which has its own interests vulnerabilities business plans etc., and hence of no real value to understanding and mitigating cyber risk

In addition, cyber space in particular is not organized by economic industry sector. Viewing this infrastructure through this "sector" lens results in a distorted and approach to cyber security in which the IT sector is viewed as a proxy for the cyber infrastructure "sector". This in turn results in an overly technically based approach to the issue rather than the enterprise-wide risk management approach that would be more appropriate and successful. So for example, far more emphasis is placed on issues such as the rapidly evolving and difficult to control technical standards compared to the more pragmatic approach focusing on human resource management to reduce the single biggest and most persistent vulnerability—insider based attacks.

Rather than government approaching its industry partners with a pre-determined organizational structure and pre-set goals and plans government ought to approach industry with a "blank page" and work on developing action plans in true partnership.

In the case of establishing industry cyber risk assessments, this alternate approach might have resulted in the private sector accessing the organizations who do this for a living, who would have provided real world data on how actual companies engage in risk measurement and broad principles could have been drawn from these (see accompanying paper on cyber insurance). This might have been more efficient and produced more powerful measures than the SCCs undertaking this program on their own, with little resources and based on a government derived and developed model.

Reasonable goals and measurable objectives for partnership projects ought to be jointly negotiated at the outset. Time lines ought to either be applied jointly to the partnership as a whole, or in instances where there needs to be separation between government and industry input timelines ought to be roughly equivalent for both partners.

4. Existing Private Sector Mechanisms Ought to be more fully Utilized

Government set the course for the one sided partnerships described above by choosing to establish its own private sector entities (e.g. Sector Coordinating councils and the Cross Sector Cyber Working Group) through which it would run these partnerships rather than relying on the many already existing private sector entities which existed.

Although these organizations ostensibly were established by the private sector, the reality is that the government decided they ought to be created, made it clear that these organizations would be the focus of the "partnership" and then provided minimal administrative support.

This left the private sector with no practical choice but to work through the government dominated organizations.

Although a committed band of individuals from the private sector have contributed substantial time and effort to these partnerships, they have limited participation from industry as a whole. Activities are overly reliant on these few dedicated individuals who represent companies with adequate resources to fund these positions (which is a vast minority of the industry) Further, many of the companies

that are claimed as members treat the membership largely as passive attempting to "monitor" the group rather than engage fully in their activities. Finally, as described above the activities are dominated by government agenda which industry representatives valiantly fight to gain parity and true partnership with limited success.

Rather than setting up their own parallel universe of private sector organizations with which to partner, thus competing with industry associations, government would more efficiently leverage the existing organizations which industry has established firm commitment to and recognizes as the appropriate industry representatives.

There are several well-established trade associations, which represent IT functions. Moreover there are several organizations representing cross sector cyber issues including the Business Roundtable, the Chamber of Commerce, the National Association of Manufacturers, and the Internet Security Alliance.

These organizations already have vastly greater reach within the private sector than the government sponsored organizations. They have a reservoir of trust, in tact professional staff, resources and a history of commitment to working cooperatively with the government.

The problem for government in basing the government's cooperative relationship with industry by using industry's designated representatives rather than through government sponsored organizations is that government would have to give up some of its "senior partner" control.

Government needs to decide if the extent of their control over the sector coordinating councils is more valuable than the expanded reach and commitment to resolving the cyber security problem which the in tact organizations would provide.

E. Evaluation Must be an Inherent Part of the Design of Partnerships

As articulated above, clear measurable goals and objectives must be an inherent part of the partnership program. The objectives for the partnership and the projects developed under it ought to be systematically evaluated on a regular basis.

Resources for evaluation ought to be included in every program undertaken and the provision of additional resources for continuation ought to be contingent on results of the evaluation.