Addressing Cyber Security Through Public-Private Partnership:

An Analysis of Existing Models

November 2009

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Acknowledgements

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Chairwoman of the Board
Frances Fragos Townsend

Cyber Task Force Members

Ellen McCarthy, *INSA President*

Charles E. Allen, *INSA, Senior Intelligence Advisor*

Stephen Cambone, *QinetiQ-North America, President, Mission Solutions Group*

Robert Farrell, *Seneca Technology Group, President and CEO*

Barbara Fast, *Boeing, VP Cyber Solutions for Intelligence and Security Systems*

Robert Gourley, *Crucial Point, LLC, founder and CTO*

Robert Pate, *Renesys Chief Security Officer*

John Russack, *Northrop Grumman, Director, Intelligence Community*

Lou Von Thaer, *GD-AIS, President*

Michael Karpovich, *INSA Staff*

Writing Team and Reviewers

Jeffrey Baxter	Scott Charney
Bryan Cunningham	Michael Delaney
Eric Greenwald	Melissa Hathaway
Jake Jacoby	James Lewis
James Longley	Joseph Mazzafro
William Nolte	Jacob Olcott
Aris Pappas	Jennifer Silk
Jennifer Sims	Matthew Stern
Anthony Spadaro	Matthew Young
Stephen Whitlock	

Editorial Review
Joseph Mazzafro

INSA's Cyber Task Force members and reviewers of this paper are senior-level business professionals with extensive knowledge and experience both within and outside of government. All joined this effort as individual volunteers and the views expressed in this paper do not necessarily reflect the views of all of the members, writers or reviewers, nor those of their respective companies or organizations.

About INSA:
INSA is the premier not-for-profit private sector professional organization providing a structure and interactive forum for thought leadership, the sharing of ideas, and networking within the intelligence and national security communities. INSA has over 100 corporate members, as well as several hundred individual members, who are industry leaders within the government, private sector, and academia. To learn more about INSA visit www.insaonline.org or call (703) 224-4672.

Executive Summary

The internet is a critical infrastructure necessary to the functioning of commerce, government and personal communication and national security. This system is not secure.

Since the nation's cyber infrastructure is not government owned, a partnership of government, corporate and private stakeholders is required to secure the internet.

The INSA Cyber Task Force acknowledges that both the 60 day study, "Cyberspace Policy Review" and the CSIS report to the President, "Security Cyberspace for the 44th Presidency" address and acknowledge the need for public-private partnership.

INSA convened a group of government and industry experts to review existing models of public-private partnerships in order to outline a way forward. They determined that while a cyber security partnership is different from others in several key ways, these models have value in defining effective partnership practices. An effective partnership has:

- A representative group of members, large enough to be sufficiently inclusive, but small enough to retain the ability to act quickly.
- A circumscribed role for government with specific tasks and responsibilities laid out clearly. Industry and private groups should take the lead.
- Properly motivated members with significant interest and stakes connected to the problem.

The Task Force reviewed the positive aspects of several models, including the North American Electric Reliability Corporation (NERC), the Federal Aviation Administration (FAA) and the United States Coast Guard (USCG).

An effective public-private partnership for cyber security would provide the abilities to detect threats and dangerous or anomalous behaviors, to create more secure network environments through better, standardized security programs and protocols and to respond with warnings or technical fixes as needed.

The Task Force sketches out a way forward in public-private partnership for cyber security, outlining two suggested components of a partnership including:

- An executive committee composed of representatives from individual, business and government organizations referred to here as a Cyber Security Panel, which represents the interests of businesses and individual users.
- A partner government organization responsible for some oversight, regulation and enforcement, focused on net security. Government is essential because only government has the authority and ability to fully investigate cyber incidents that may occur across networks and only government has the ability and legitimacy to regulate industry where private citizens' interests are at risk (as with privacy).

Other components that may be included:

- Inspection and enforcement of standards upon suppliers and Internet Service Providers (ISPs).
- Ability to watch networks, searching for and analyzing future threats and warning all users before an emergency occurs.
- Ability to respond to attacks, through warnings and technical fixes, as well as plan for the recovery of crucial systems after an emergency.
- Necessary protection for privacy and free speech, individual rights and business concerns, cognizant of government needs. Resulting implementation should work toward collaborative solutions.
- Mechanism for international collaboration on cyber security.

The Task Force recognizes there are a number of ways to address cyber security and believes the effort to do so should begin right away on three fronts: private sector self-regulation, executive branch leadership and congressional action.

Introduction

In light of the White House 60-day review of Cyber Security and that effort's call to improve public-private partnership, INSA convened a group of government and industry experts to review ways to improve cyber security for all users. This group agreed that, given the origins and character of the internet and its centrality to the conduct of private and public affairs, a partnership could serve to assure access to and the performance of the internet through improved cyber security while being respectful of users' privacy.

Nearly every facet of modern life is connected to the internet and the associated wireless environment in some way. We, individuals, business and government organizations, are all at risk to the prolific threats impacting our networks. Malicious software and ruthless hackers can travel undetected to any location benefiting from the near absence of security between independent network owners. This lack of coordination across the public and private sector leaves the user vulnerable to malevolent behavior that, among a long list of possibilities, can invade their privacy, steal their identities, deny critical services, or create conditions in which public confidence in governmental institutions is diminished.

Laws, standards and technology cannot simply be levied against such an integrated system of networks. Questions over roles, responsibilities, and jurisdictional boundaries only become more prolific as we strive to clarify them. The health and abilities of one affect all others. This is complicated by the reality that this is ultimately a global network. Governments, businesses and citizens are all affected by negative market reactions, liability exposure and unwanted release of proprietary and personal information.

Developing the Model (Methodology)

In recommending a partnership model for cyber security, the INSA Cyber Security Task Force reviewed ten existing public-private partnership (P3) models currently operating in the United States. Brief descriptions of the P3s we examined and their potential relevance to the creation and operation of a P3 for cyber security are in the appendix. The list is by no means exhaustive, nor was it meant to be. The list was intended to provide a sufficiently large sample size to provide an "existence proof" that P3s address successfully complex problems today and might be a way to address the complex problems associated with cyber security.

The P3s chosen for inspection contain, to a greater or lesser extent, features we believed might serve well if incorporated into a cyber security partnership. They also feature greater and lesser roles for government. But what attracted us in each case is that the role for government has been carefully circumscribed—by law, regulation, policy, incentive and practice—such that the public interest is met without the imposition of onerous burdens—e.g., taxes, operating limits, regulations—on the private sector.

We, individuals, business and government organizations, are all at risk to the prolific threats impacting our networks.

It is important to note that a cyber security P3 differs from historic partnership approaches in several key ways and thus that these efforts, while informative, require some adaptations to the cyber realm. The Task Force identified three attributes unique to a cyber security P3 that engender some complication:

1. Issues of property in the cyber realm, both intellectual and in asset valuation, may not have direct parallels to existing concepts of property addressed in other P3s.

2. Other P3s operate under established regulatory structures built around a variety of local, state, federal, international and mixed authorities. Such a set of original authorities does not exist in comparable degree in the cyber domain. Companies have been, and may remain, unwelcoming to the idea of regulation on the internet, but internet security is a national need and government has a role in providing for this need. On the other hand, regulation as it has been practiced in unlikely to fulfill this need while meeting user expectations. Hence, the partnership model is the most effective way to improve security while circumscribing the role of government and meeting the specific needs of users. The lack of a basic regulatory structure and the need for a new system is a rare track for the development of a public-private partnership and may lack historical example.

3. The time scales involved in cyber development, incident, response and threat indications are all vastly shorter than anything in other P3s.

For these reasons and others, no one public-private partnership provided all of the desired features, but all of the examples had one element in common. They represented a commingling of private interest in securing the public good and public (i.e., government) interest in advancing private sector capability in response to publicly acknowledged needs or dependencies.

To be effective, we judged that a model partnership would need to represent the interests of parties whose concerted and agreed behavior can produce the desired outcomes. This means that the partners must be:

- Broadly recognized as having a sufficiently high stake in and motivation or incentive to improve the security of the internet.

- Able to demonstrate that in advancing their interest they are also advancing the wider public interest.

- Sufficiently few in number to operate effectively, but at the same time broadly representative of and capable of influencing the behaviors of the constituent elements of the partnership.

The constituencies to be represented include:

- Suppliers—this constituency can be nearly as broad as the user set, depending on the purpose of the partnership. The makeup could range from content suppliers, Internet Service Providers (ISPs) and software and hardware producers to telecommunications companies (telecoms), etc.

- Users—ordinarily thought of as individuals, but which include small and large businesses, organizations, associations, etc., as well as government entities. These users are both domestic and foreign.

- Government—Government has two important and distinct roles. Firstly, it is a regulator of the market in its role as the protector of public interests. But secondly, it is a massive consumer of internet services and is heavily dependent on those services to communicate with and provide for its citizens. The choice of government partners is critical to ensure that the these roles are balanced and desired authorities are inherent in the mission of the partnered agency, but at the same time its reach is sufficiently circumscribed such that it cannot operate effectively without the voluntary cooperation of the users and suppliers.

Our review narrowed the number of existing P3s that met these criteria to three whose characteristics we thought might be incorporated into a cyber security P3:

P3 Model

		Interests	Capabilities	Limitations
Telecommunications companies, Software and Hardware Suppliers and Internet Service Providers (ISPs)		Want to deliver services and protect the privacy of customers Want to be reliable suppliers: optimal performance is just as important as permanent availability, perhaps more so Must be assured that regulation will not stifle development and disadvantage them in economic competition	Have specialized technicians able to identify abnormal activity quickly Are well-positioned to block 'downstream' attacks Are well-placed to distribute security software to their customers and enforce standards through connection agreements with subscribers	Are reticent to involve themselves too deeply in security info-sharing due to privacy and liability issues Would likely be unwilling to incur higher costs for security
Government in role of regulator		Want reliability and protection to ensure critical infrastructure protection Depends on the integrity and protection of internet transactions to protect the privacy of citizens and the economic well being of the country	Can provide a necessary legal enforcement role for cyber security Can also provide a platform for international action and outreach Can provide incentives to encourage greater participation in cyber security P3	Have difficulty coordinating response across large bodies Have fractured and diffuse authority Are hindered in ability to share information by classification processes Security provision may conflict in some cases with privacy concerns
Users: large corporations, small businesses, individuals, Information Sharing and Analysis Centers (ISAC), government and private organizations, and academia	Individuals	Want accessibility on demand Need greater protection of personally identifiable information and personal computers Are suspicious of government role on the internet and would require strict rules and strong oversight for regulators	Have large numbers of machines that could possibly be used to voluntarily collect and distribute information regarding potential or actual attacks	Are often unaware of cyber security risks Are untrained and unaccustomed to guarding against attacks
	Government	Depends on availability of the internet to provide public services, communicate, store and access vast amounts of information and to support national security operations	Have large networks that are already tracked for threat information, a useful dataset for threat analysis	Adopt newer, safer technology slowly Does not coordinate responses well
	Businesses (small businesses fall in closer with individual users)	Want accessibility on demand Have a strong interest in secure networks to advance e-business and safeguard communications and protect proprietary and competitive data. Must be assured regulation will not adversely affect business and innovation	Often have sophisticated security organizations or contract out to security providers Share information through industry trade associations, standards organizations and government liaisons Participate in the development of standards	Adopt new technology and practices more slowly as the size of the institution increases Have limited participation in info sharing due to privacy and liability concerns

Analysis of Existing Models

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)

The NERC began as a private, voluntary organization, established by the companies that supply electric power to the electrical grid of the United States and Canada. In an effort to guard against the causes and effects of regional blackouts and other major service disruptions that are harmful to their business, the suppliers agreed on an enforceable set of standards related to their operations.

NERC's user partners are their customer organizations and regional contemporaries with whom they contract for the delivery of service. The standards serve to codify what each firm in this highly interdependent market can expect from one another, since the failure or negligence of one supplier can adversely affect other responsible companies. The terms and conditions of contracts between these bodies stipulate compliance and thus serve as the mechanism for creating the behaviors among the suppliers.

For a period of time the NERC acted entirely as a voluntary organization. Eventually the Federal Energy Regulatory Commission (FERC) sanctioned the NERC standards and standard making process as federal regulations. This was done to gain government input on the standards-making process for the purpose of protecting infrastructure, the NERC agreed because it gave their standards a better mechanism for enforcement.

This partnership has the suppliers—energy companies of all types—select a board of governors, take input from their constituent elements and users and fashion standards of behavior and conduct which are subsequently adopted by the suppliers and reinforced by federal regulation.

THE FEDERAL AVIATION ADMINISTRATION (FAA)

The FAA differs from NERC in that it is a federally founded organization designed to protect consumers by ensuring flight safety. Because aviation is now international in character, FAA regulations have grown in importance to affect the behavior of airline manufacturers and operators outside the US, as well as foreign governments.

While the FAA does not have a "user" constituency, per se—the customer—the well being of the user, in this case airline passengers, is an interest of the government and is the major impetus behind the FAA's regulations.

The mandate of the FAA is sufficiently circumscribed. It has wide ranging authority to issue directives affecting the manner in which flight operations are conducted, the operators (airlines, pilots, mechanics, etc.) are licensed and evaluated, aircraft are designed, deemed flight worthy and modified, and is party to accident investigations. FAA authorities are designed to advance the safety of flight and with it the interest of the suppliers and users. The former has significant influence over the activities of the FAA and both are very much interested in maintaining the confidence of the user community.

THE UNITED STATES COAST GUARD (USCG)

The Coast Guard is a venerable institution whose origins—as a U.S. government (USG) agency enforcing customs duties—would seem the antithesis of the kind of privately motivated partnership we are advocating. Yet, as it evolved into its current form, it was successively assigned a number of roles that are consistent with the approach we are proposing. Like the FAA, the USCG has an interest in safety, assuring that vessels are seaworthy, licensed for inland waterways, and operated according to regulations designed to ensure safe passage. It fulfills this role through cooperation both with boaters and operators, through free public certification classes or public information and feedback sessions, and with port authorities and manufacturers, through prefabricated agreements on safety measures, jurisdiction and point of manufacture inspection.

True to is heritage, the Coast Guard has retained its law enforcement role. While its enforcement powers are wide ranging, dealing with immigration, trade, drugs, fisheries and general public safety, this role is confined to a limited and specific geographical space: the nation's coastal and inland waterways.

The Coast Guard also has a national security role. It can be called into the military by order of the president under prescribed conditions and assigned combat missions both in US and foreign waters.

While not specifically a partnership, the Coast Guard demonstrates that continued engagement between regulators and users can allow a regulatory body to simultaneously address issues of many types and of different magnitudes such as personal safety, law enforcement, and national security.

THE MISSION OF A CYBER SECURITY P3

The mission of the proposed partnership, broadly defined, would be to establish reasonable standards and best practices such that anomalous activities and behaviors could be identified. This identification would then allow for notification (provided to users and suppliers alike) of the existence of these behaviors and vulnerabilities across processes and technology, enabling remedial action to minimize or prevent loss of assured access or privacy for users.

To be effective the P3 would need to provide three capabilities essential to cyber security:

1. Detection: The partnership must define, identify and watch for behaviors of concern

2. Protection: It must ensure compliance with the partnership's security standards, sanctioning those who fail to comply.

3. Response: It must provide a means to conduct forensic examinations following disruptions, analyze vulnerabilities, fix security shortcomings and effectively attribute attacks to their perpetrators.

These activities, as well as incentives for greater participation and sanction for failures in conduct, would need to be agreed to and accepted by all parties: suppliers, users and government.

Recommendations and Model

A CYBER SECURITY P3 SHOULD POSSESS THE FOLLOWING ELEMENTS:

Cyber Security Panel (CSP)

Establish an executive committee composed of representatives from individual, business and government organizations. Building off of the NERC model, the existing Information Sharing and Analysis Centers (ISACs) could appoint a Cyber Security Panel, to sit with representatives from the ISPs, to establish the standards for definitions for anomalous behaviors, the requirements upon suppliers and methods for response to anomalies, by both users and government, which in their judgment could lead to a more secure cyber environment.

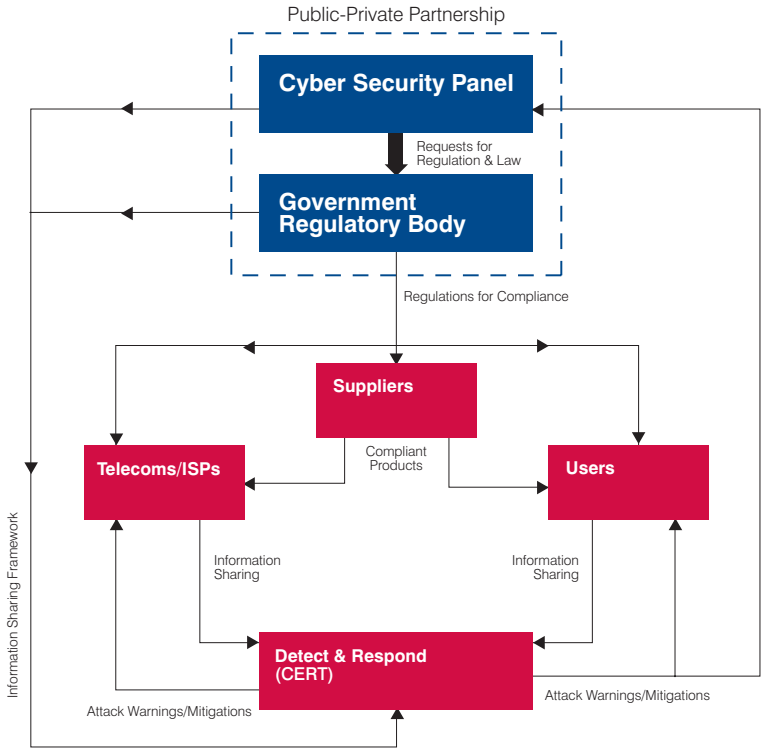
Representatives of the public interest or users could be added to the mix, creating a tripartite organization of public-private interests. These public representatives might be appointed jointly by Congress and the President. In all, the CSP should not exceed a number needed to be sufficiently representative of all the interests but at the same time capable of conducting business. To assure its continued connection to the interests it is intended to represent, provisions could be made for term limits for members and staff.

This process would closely track with a common organizational structure of Public Utilities Commissions (PUCs), another model assessed by the Task Force (see appendix). While some may contend what positive impact the PUCs have had on the utilities sector, they have been successful in protecting the interests of private citizens in the realm of utility services and prices through the inclusion of appointed or elected representatives of the public interest. This may be another model worth emulation.

Regulation of Suppliers

ISPs, telecoms, software and hardware manufacturers could follow some combination of the FAA and NERC models for the regulation of suppliers. Security programs and protocols could be standardized by the CSP, but in the spirit of the FAA, the direct impact on the user could be limited by regulating the users via their suppliers.

A graphic and conceptual representation of a possible system for cyber security partnership.



It is with good reason that users resist explicit measures that would impose standards upon behavior on or access to the net. Rather than court controversy, a useful step might be to require only that a user demonstrate that the device on which network access is sought meets a minimum standard of "net safety." That is, it has an up-to-date security suite. This requirement is already in force for many businesses today for remote access and is also required by many ISPs before they will engage in "correspondence" with a user, i.e., download software. It is hardly a perfect solution, but like a boating certificate from the Coast Guard or flight worthiness certificate from the FAA—both of which are interested in safety, not who is boating or flying—it sets a minimum standard for reducing risks associated with inappropriate or malicious behavior.

To ease this burden, the suppliers of software and hardware products could be advised of and included in the production of these standards for their component parts. Thus all component products on the shelves would be able to carry built-in baseline security compliant with the ISP and telecoms' standards. While not a perfect solution, this could be a start for security collaboration and interoperability measures that could advance the safe operating of the network.

Inspection and Enforcement of Suppliers

These functions might follow the FAA model, which emphasizes self-inspection and self-reporting to leverage private sector expertise and lower regulatory burdens. This approach is animated by safety of flight, not the business of building and flying aircraft. It is focused on assuring the enormous economic opportunities created by public assurance that flying is safe. It is not directly concerned with the reason a user has for flying. Nor is it, except for forensic reasons or in response to statute or regulation unrelated to flight safety (as in the case of watch lists), interested in who the users—passengers or other paying customers—may be. And within limits (again related to flight safety) it is uninterested in what a passenger does on board an aircraft.

Hence, in its approach, the FAA does not act as a law enforcement agency. The FAA allows airlines to inspect their own operations, but retains authority over the process by requiring these inspectors be certified by the FAA. But the airlines ignore the instructions of the FAA at their peril—less from an intrusion by the FAA into their affairs on a daily basis, than by the consequences of a flight failure stemming from lax reporting or a failure to follow FAA instructions.

Just like the FAA, this proposed partnership could allow for self-inspection for compliance and count on its disciplinary procedures after the fact and the business that would be lost as a result of safety failures to ensure responsibility.

As an alternative, or in addition, one might look to the Coast Guard model for inspection and enforcement. For example, it has a regulatory role related to boating safety and safe conduct on the sea. But it also has circumscribed authority to conduct law enforcement, monitor and survey, gather intelligence and respond to hostile action. It has a domestic as well as international role and presence.

There may be value, however, in separating the inspection and enforcement of standards—non-criminal in nature—from law enforcement or national security actions. Without this separation, fear of prosecution may color the private sector's assessment of the security partnership, limiting participation and enthusiasm if they feel failure to comply with standards may be viewed as a criminal offense rather than an administrative issue.

Mitigation of or response to anomalous behavior or malicious acts might draw further on the Coast Guard model. It has highly specified roles and responsibilities. It has both a domestic and foreign role. It can operate under a wide variety of civilian and military (and intelligence) authorities closely tied to its roles and missions.

As noted these three existing examples hardly exhaust the features that might be drawn from other organizations and incorporated into a public-private partnership. Following is a brief description of other characteristics from existing entities that might be considered in developing a partnership-centered cyber security regime.

Watch and Warn

This function is essential to internet security. The National Weather Service (NWS) engages in this practice continuously. The virtue of the NWS model is that it employs publicly supplied tools to watch or monitor the weather in the belief that knowing the state of the weather is a public good. The NWS, however, takes no responsibility for the actions taken (or not) in response to its warning. Nor is it held liable for its failure to predict accurately. Nonetheless, a loss of the service would be dearly felt by the public. A cyber security partnership could, likewise, have an element that performs this function without liability.

An additional possibility is that the suppliers of internet access—the ISPs, likely in cooperation with the telecoms—could agree to baseline standards for security measures as part of user agreements. This would provide the mechanisms and tools that would allow the partnership to perform the functions necessary to watch for anomalous behavior, detect vulnerabilities, warn users and take remedial action. The P3 would need to set the standards for system security and

performance, stipulate thresholds of reporting, and ensure the distribution of information that, analogous to the FAA interest in flight safety, could affect "net safety."

Government could extend requirements and best practices to its contractors via the terms and conditions of contracts as well as procurement guidelines. Coupled with the self-inspections above and agreements on shared costs and risks—the latter implying that in return for self-inspection data the government provides contractors with up-to-date threat data to modify control systems, etc—the partnership could reduce unsafe behavior and safeguard national interests at the same time.

Response and Recovery

An effective system for cyber security could, in addition to the ability to watch and warn, contain a mechanism for developing responses to problems as or before they develop. The monitoring discussed above could be leveraged to create or supplement a standing analytical capability, scientifically assessing threats and searching for solutions to mitigate their effects or consequences. This would allow for immediate response, in the form of precise, detailed warnings, as well as rapid-acting and technically-advanced system recovery planning. These functions could be augmented by a series of "red-team" exercises, building off of the momentum and know how generated by the annual 'Cyber Storm' exercises held by DHS. This would generate forward thinking and threat anticipation that could lead to more rapid and effective immediate responses and more productive recovery planning.

Protection of Privacy

Privacy and civil liberties interest groups, and many individuals, are uncomfortable with significant increases in the government's ability to investigate, collect information in an unfettered manner about, and regulate or otherwise interfere with, private activities on the internet. The most significant concerns in this area concern potential government access to intimate discussions, expressions of political dissent and protest intended to be private, and Personally Identifiable Information (PII). Privacy and civil liberties groups worry both that the government, if not sufficiently checked by strict regulations and court and congressional oversight, will collect such information without appropriate approval and limitation and will repurpose or otherwise misuse the information. Broader still, privacy and civil liberties groups worry that, even in the absence of any government misconduct, the very fact of increased governmental monitoring and control of the internet will "chill" speech and activities protected by the United States Constitution.

Finally, these same groups, as well as business and economic interests and cyber industry professionals, worry that increased governmental regulation will be ill-informed and ineffectual or even counterproductive. They worry that governmental actions will stifle economic and technological progress and advantage economic competitors in nations with less internet regulation.

These legitimate concerns must be addressed, and this issue may be central to any effort to secure cyberspace. The partnership will almost certainly require some means to protect the privacy and speech rights of individuals while maintaining adequate security for all users and not stifling business innovation. A partnership approach is well suited to this task, as its inclusive membership can adequately represent the need the government has for some enhanced access to private and commercial information, as well as the interests of all sides, avoiding the false dichotomy between security and privacy to reach some sort of collective solution. These potential solutions could include, automated processes for monitoring, analysis, and response mechanisms, including the use of anonymization and related technologies and stronger procedures and policies for oversight.

International collaboration

Because the internet and the business and communications functions it supports are global, the international dimension of cyber security needs attention in any partnership. Here again, existing arrangements might be consulted.

In reference to the safety of flight discussion, the international community did establish the International Civil Aviation Organization (ICAO) as a UN agency in 1947. While it has an international mandate, its capacity rests on the national aviation agencies. Additionally, the Council of Europe's Convention on Cyber Crime Treaty has been effective in aligning international actors to fight cyber crime and might be a useful example.

US Government Participation

In proposing a public-private partnership for cyber security, we have focused our attention on the participation of the private sector. Much of the foregoing could be self-generated and self-imposed by the private sector based on a strong value proposition and market-based incentives.

However, two considerations militate against such a proposal. First, the private sector, even if represented by the full range of "users" identified earlier, does not have the legitimacy to regulate in cyber space, especially in those instances where such regulations affect the privacy rights or interests of individual US citizens. Only the government, appropriately constrained by law, possesses such legitimacy. But even it must tread carefully on this issue in practice

Second, only government, constrained by law, can fully investigate the behavior of individuals or groups, apprehend, prosecute and punish those who violate the law or defend against and respond to threats and attacks against the nation's interests.

Hence, a government sponsor of the partnership is needed. Under current arrangements, that role would fall to the Department of Homeland Security, most likely the National Protection Programs Directorate (NPPD).

Under the approach described here, we would imagine a dialog between the tripartite CSP and the NPPD in which the panel presented its approach to cyber security. This dialog could identify the limits of self-generating and self-imposed behaviors and sanctions, describe the reinforcing but carefully circumscribed role that could be played by the USG in support of the partnership and provide a prospective list of agencies whose existing authorities and approach to its regulatory role would render them valuable government partners in advancing cyber security.

For its part the USG partner would undoubtedly seek to define the public interest, establish the existence of or need to create a new legal foundation for the P3, determine its own role, broker arrangements with other agencies whose interests were affected and assess the need to create new authorities in existing agencies or create new agencies. It could then approach Congress through the office of the President to gain their participation and blessing.

We would imagine that such a process would not reach a conclusion at once. Indeed, an effort to do too much at once would inevitably fail. A time and performance based approach, in which those elements of cyber security on which most agree could be brought to bear first, might provide a sound base for progress.

Conclusion

The foregoing is not meant to be exhaustive but illustrative of the potential for using existing P3 elements to address the cyber security issue. The problem that remains is how to initiate such a partnership.

One possibility is a private initiative, most likely led by the ISPs and telecoms, to prepare a charter for a cyber security partnership organization and initiate a discussion with a government sponsor. INSA is prepared to offer its good offices to assist in such an initiative. Another is through Presidential initiative, tasking DHS or a federal agency to take the lead. A third is by Congress, which might establish a public broadcasting-like organization to take the lead.

Public and private actors face unprecedented and unacceptable risks on the internet today. This system is a critical mechanism for business, government and personal communication and must be safeguarded. Whichever approach is taken, it is crucial that someone take ownership of the problem and begin to address it in a systematic manner, through a partnership of all stakeholders. This approach has successfully addressed complex national problems before, as the preceding study shows, and can continue to do so. Indeed the Task Force believes it to be the most promising route forward and INSA is eager to assist any body, public or private, that aims to advance cyber security through effective public-private partnership.

Appendix: List and Summary, all P3's considered

Federal Aviation Administration (FAA): The FAA regulates nearly all aspects of travel by air. They establish technical, personal and organizational standards in close cooperation with the airlines and monitor and direct flight traffic. They also make effective use of industry resources by allowing for airlines to inspect their own operations.

+ Establishment of universal standards for operators, performance, maintenance and safety, developed as a result of a collaborative process easily maps itself to the internet and added value for the airline industry. Also, the self-regulation structure engages and partners effectively with industry.

- The tracking of traffic and user identity is much more problematic on the internet than in the skies and the close regulatory relationship between the FAA and airlines sometimes results in poor enforcement.

The North American Electric Reliability Corporation (NERC): The NERC is a private organization that brings together all the major providers and transporters of bulk power. While developed outside the government, they have been sanctioned by the Federal Energy Regulatory Commission (FERC) to establish standards for the bulk power sector. The NERC members agree on standards and best practices for their industry, with input from FERC, monitor power transit infrastructure, plan for future changes in the industry and undertake self-monitoring and enforcement, though FERC can also penalize violators.

+ This model provides a picture of a non-invasive, effective and industry-led effort that recognizes the demands and constraints of standards on the business community. It also shows that a monitoring, investigation, warning, emergency response and readiness maintenance process can be situated in the private sector and regulate the market effectively. Under this system, industry standards remain business-centered, but meet the government's security requirements.

- The consensus process used to reach new standards is slow and tedious. Cyber standards must be able to adapt to a rapidly changing environment and day to day management functions are sometimes handled by committee further slowing processes. Finally, the dual role of NERC as strategic planner for the industry and regulator has caused confusion, misaligned interests and opaque proceedings.

The United States Fire Administration (USFA): The USFA is a research, warning and education center for the firefighting efforts of the nation. They used a standardized fire-reporting system to gather massive amounts of fire data and put this data to use conducting research on fire-fighting techniques and fire trends and providing educational material and training to firefighters across the country.

+ The technology, research, training, and incident reporting found in USFA are good examples for cyber. The USFA paints a clear picture of the state of firefighting and gives firefighters the tools to be more effective. This model could be followed in cyber, training and equipping cyber professionals to keep them up to date and prepared for the newest iteration of the cyber threat. The National Fire Incident Reporting System (NFIRS) is a great example for standardized reporting that leads to greater value delivered.

- The USFA exists to empower existing bodies and this is not the best approach for cyber. Confusion already exists over jurisdictions, roles and responsibilities and further empowering these disparate parts could exacerbate this problem. Crucial differences also exist between fires and cyber incidents which lessen the usefulness of this example. Cyber attacks are more easily concealed from the public than fires. If one could conceal these fires from customers and constituents, one must wonder if they would be reported. Also, fires are often unintentional and almost never coordinated for maximum impact, and the USFA structure may not be up to the rigors of the cyber dilemma.

Public Utilities Commissions (PUCs): The internet is increasingly viewed on par with the telephone, electricity and other PUC-regulated markets as a modern communication and commerce necessity and the PUCs have been effective in regulating and helping secure crucial sector markets for nearly 100 years. Through a decision-making and regulatory body split between producers, consumers and government, empowered by the state, PUC's regulate pricing and service to assure affordable access to users and a profitable environment to suppliers.

+ The historical development of PUCs gives us a model for government leadership coupled with business community input and participation to form an effective partnership. Several of these PUC constructs may show a way forward in forming cooperative decision making bodies that will be required in the field of cyber security to finding mechanisms for regulation and protecting the interests of individual consumers.

- PUCs generally regulate big picture consumer-supplier issues such as pricing, service, monopoly protection etc. They have shown little ability to coordinate and lead action amongst their member groups, instead generally acting as mediator and arbitrator between them.

The National Oceanographic and Atmospheric Administration (NOAA): The NOAA is a collection of previously independent agencies that operate together for the purpose of providing greater knowledge about the oceans and weather, and preserving the nation's living resources.

+ The structural fusion of situational awareness organizations (such as the National Weather Service and National Ocean Service) and enforcement bodies (like the Fisheries service) create the ability to better aid security on the internet through cooperation and information sharing with regular, standing law enforcement and various other private organizations.

- The NWS is a good example of awareness provision, but the model, strictly interpreted, cannot be applied effectively to cyber. Widely sharing threat information publicly would introduce new vulnerability. Additionally, the time frame of these warnings is usually measured in hours, which is not likely to be enough time to coordinate an effective response. Lastly, the NWS model is not designed to compete against cognizant actors; prediction systems are governed by scientific analysis and while this may be useful to predict future net weaknesses, this system is not a match for the cyber dilemma.

National Institute for standards and Technology (NIST): NIST is a federally funded research organization that houses scientists and academics who seek to objectively identify the best standards and business practices, to advance the economy of the United States. NIST already has a considerable role in cyber security, developing and implementing federal agency's FISMA guidelines.

+ NIST is well-position to serve as a conduit between business and government, allowing for cross-consultation and the development of best practices and standards across private/public lines.

- NIST has no enforcement powers or mechanism. Giving these powers to NIST would fundamentally alter their operating pattern as a scientific, organizational and industrial research organization.

United States Geological Survey (USGS): The USGS is a permanent, scientific monitoring organization providing constant awareness and studying future developments in the field of geology. They monitor seismic activity and earthquakes in order to predict and prepare for emergencies and also provide detailed mapping services, among other functions.

+ USGS assesses present threats, anticipates future problems and publishes the information in real time. In cyber this would greatly increase awareness of the threat of cyber attacks and help the government and private sector prepare for the next incident.

- This sort of arrangement may also broadcast vulnerabilities and responses to too wide a net, including those responsible for the attack, severely limiting its usefulness. Additionally, it has no enforcement mechanism.

The Civil Air Patrol (CAP): The Civil Air Patrol is non-profit, volunteer organization that acts as the official auxiliary service to the United States Air Force. They also fly missions in support of disaster relief efforts, search and rescue and law enforcement operations. Many of their members gain valuable flight time and pilot's certifications from their membership.

+ The aspect of the CAP that most stands out in relation to cyber security incident response is the organization's flexibility. The resources and effort of the CAP can be seamlessly shifted between missions of emergency response and recovery, national security and law enforcement as needed. This is a strong model for cyber, where these roles constantly intertwine and overlap. The CAP also trains new pilots, and training new cyber security professionals could only serve to improve cyber security.

- The use of volunteers is most likely infeasible in cyber, as it could introduce new vulnerabilities. Also, the CAP lacks standing authority; instead it is empowered in the event of special circumstance or emergency by another body, borrowing on its authority and mission.

The Coast Guard (USCG): The Coast Guard is a military service branch tasked with the defense and maintenance of the nations waterways. They are at different times a military, regulatory and law enforcement body with wide powers in the territorial waters of the U.S.

+ This body is very flexible and equally able to address law enforcement, security, personal safety and market concerns as needed, which is vital on the internet where the lines blur easily.

- But the wide ranging authorities the Coast Guard possesses are to a large extent accepted as part of the maritime playing field because they have almost always been there. Granting similar powers to an agency in cyberspace would almost certainly run afoul of the accepted free, unregulated and anonymous culture people have come to expect from the internet.

Department of Transportation (DOT): The DOT is a federal agency tasked with regulating the national highways and railways. It sets standards, helps direct private resources and plans nation-wide transportation systems.

+ The DOT example shows that a strong government-led department can regulate, leverage and structure private industry resources to improve a critical network.

- The historical development of the highways and railways occurred with DOT's influence (or some federal equivalent), and the internet has already matured without this regulatory structure and it is doubtful a DOT-like arrangement would have the same power, influence or efficacy. Its top-down approach also imposes rules and requirements on businesses from the outside instead of engaging in partnership with them to make sure the incentives are well ordered and the system makes sense.

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Intelligence and National Security Alliance
901 North Stuart Street, Suite 205
Arlington, VA 22203
Phone (703) 224-4672
Fax (703) 224-4681
www.insaonline.org