



INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Critical Issues for Cyber Assurance Policy Reform

AN INDUSTRY ASSESSMENT

Executive Summary

Cyber assurance is a critical issue for the United States. There are many technical and policy issues associated with providing an acceptable level of cyber assurance for our government and commercial infrastructures. Solutions to many policy issues are unclear and not easily defined. To take action, the President commissioned a comprehensive cyber assurance study in order to identify public and private sectors that have a stake in cyber assurance, pose key questions to frame the relevant issues, articulate concerns, and formulate initial policies for our nation in this critical area. The Intelligence and National Security Alliance (INSA), which represents the defense, intelligence, national security, and telecommunications industries, formed a task force to address several of these questions.

INSA worked with members of the defense, intelligence, national security, and telecommunications communities to address these questions (Appendix 2 lists contributors). All contributors are senior professionals, with years of experience that span the technical, managerial, and policy aspects of their industries and the public/private partnerships that exist today. These individuals provided their personal and professional time to give expert advice to create the policy recommendations in this document. These opinions are not attributed to the member companies, but are the outcome of free and vigorous discourse between senior professionals with diverse experience presenting their personal views and ideas.

The INSA team used the following question sets to frame the discussion and debate:

1. What is (or should be) the government's role in securing/protecting the critical infrastructures and private sector networks from attack, damage, etc. (from nation states)?

- What are the minimum standards that must be established?
- How will these standards affect procurement/acquisition policies?

2. Much of the success of the current Internet architecture stems from the fact that the architecture ensures there is a unique, authoritative root.

- How would the security and stability of the Internet be affected if the single, authoritative root were to be replaced by a multiple root structure?
- What would be the economic and technical consequences of a multiple root structure?
- What, if any, influences do you see that may:
 - Move the Internet in the direction of greater fragmentation; or
 - Help to preserve and maintain a single, interoperable Internet?
- What are the implications of these forces?

3. Our lifestyle is based upon a digital infrastructure that is privately owned and globally operated.

- How do we get to a public/private partnership and action plan that will build protection and security in – and enable information sharing to better understand when it is under a local or global attack (warning)?
- What is the model public/private relationship?
- Who and how will oversight be conducted in the IC and national security community?
- How would you provide common situational awareness?

It is important to note that regardless of the policy recommendations that are made in this paper, providing complete cyber security in today's world is a difficult technical problem. The government must continue to invest in technical improvements to the science of cyber assurance. New policies and procedures are important but are all predicated upon continuing improvement in the technical capabilities of government and industry to defend their assets.

In this paper, the INSA team provides many ideas and recommendations that serve as starting points for crafting new and improved cyber assurance policies. There are several common ideas and approaches resulting from

Question One

these three questions that stand out as primary areas to be addressed and attacked first. The basic report covers the specific recommendations that grew from the common areas within these questions.

Key areas to address are:

- In clear and concise detail, define who is in charge of national cyber assurance and what their specific authorities, roles, and responsibilities are inside and outside the government.
- Create an effective public/private partnership with a twofold purpose. First, insure that industries receive timely information that will enable them to react to attacks. Secondly, provide industry with protection when it reveals proprietary and sensitive information to government and competitors about attacks, penetrations and their infrastructures.
- Aggressively undertake the government's role of educator, standard setter, compliance auditor, and law enforcer.

By focusing future policies on addressing these issues, a more effective public/private partnership and national cyber assurance process can be created that better serves government and industry needs. These recommendations provide politically feasible and practical solutions, which aim to address key problems of the defense industrial base, critical infrastructure sections, and our national information infrastructure.

We look forward to working with the government in the establishment of new standards to mitigate advanced cyber threats.

What is (or should be) the government's role in securing/protecting the critical infrastructures and private sector networks from attack/damage, etc. (from nation states)?

- What are the minimum standards that must be established?
- How will these standards affect procurement/acquisition policies?

Discussion

The government's role in protecting and securing the nation's critical infrastructure, which is 85% privately owned, should be to first focus on the core, truly critical sectors to national security and to work more effectively with the private sector to protect those critical sectors. We recommend that communications, power, transportation, and finance are the critical starting points.

The owners and operators need to have a greater understanding of the threats to these critical sectors and consequences of failure. The government needs to significantly improve their working relationship with the Center for Intellectual Property (CIP) owners and operators. The government should also make necessary revisions and adjustments in law, policy, liability, and enforcement as we move forward. Additionally, the government must set minimum standards for protection and enforcement of these standards. A national cyber recovery plan should also be developed to address cyber response from a large-scale cyber attack.

A single cyber security official should be appointed at the White House-level to clarify the roles, mission, and responsibilities of those government agencies involved in CIP. The responsibilities of this individual shall include the development of the national cyber security plan and organizing our nation to effectively function through a cyber attack.

All parties must drastically improve information sharing amongst their organizations. This includes examination for and removal of impediments to information sharing and an improvement to the method for sharing, where appropriate. Lessons learned, best practices, and threat information should be provided by the federal government to the private sector as "real value added" and should be easily understood and appropriately tailored to the sectors. Speed and timeliness of information sharing needs significant improvement for the achievement of a successful desired degree of protection and attribution.

Vast improvements need to be made in real time advanced analytics for attribution. This includes removal of the legal and policy impediments to getting the data and information necessary to do attribution. Data access and knowledge management also need significant improvement if we are to ever get to the unambiguous standards required for attribution. The technical tools and applications necessary to do the advanced analytics required for attribution require investment from both government and the private sector. Laws, regulations, and standards of behavior in cyber space must be reviewed and strengthened so that law enforcement can conduct much more effective investigations and apprehend and punish those responsible.

Protection of our nation's critical cyber backbone is achievable if we have the empowered leadership, focus on what is truly critical infrastructure, provide a full understanding of the threat, and improve information sharing and situational awareness between all parties involved.

Minimum Standards to Establish

Partnerships and standards between the government, industry, and the private sector are imperative for cyber defense. One highly successful example of effective standards is the Capability Maturity Model Integration (CMMI). This model grew out of a public-private partnership between the United States Air Force (USAF) and the Carnegie-Mellon Institute in the 1980s. The partners created CMMI to address a similar pressing national issue arising from software development risk.

The National Institute of Standards and Technology (NIST) develops standards and guidelines for complying with the Federal Information Security Management Act (FISMA). NIST produced a comprehensive set of recommended security controls developed by a group of government and private sector organizations. NIST recently released for review a major update of the guidelines, **Special Publication 800-53**, titled "Recommended Security Controls for Federal Information Systems and Organizations." We are aware of two private sector efforts, both threat oriented, intended to complement the work in NIST 800-53:

1. Consensus Audit Guidelines (CAG)¹. The CAG, recently released to the community for review, identifies twenty security controls and metrics for effective cyber defense and continuous FISMA compliance focusing on leveraging the standards and automating assessment methods available in the industry. This document intends to begin the process of establishing a prioritized baseline of information security measures and controls that address defenses against attacks. The CAG intends to complement NIST 800-53 and to aid auditors by identifying the areas that auditors should focus on first when evaluating the progress of an organization's cyber security efforts.

2. Cyber Preparedness Levels². This activity categorizes five levels of cyber preparedness, including three specifically intended to correspond to the advanced cyber threat. Each level assumes a different level of cyber threat against which an organization has to prepare. Associated with each threat level is a listing of security controls that are intended to counter identified threats. The objective of this effort is to provide organizations a means to facilitate cyber security investment management and planning decisions.

NIST plans to incorporate the Cyber Preparedness Levels into both its security controls and risk management guidelines. While both threat focused, the CAG and Cyber Preparedness

¹ The CAG was developed by John Gilligan in cooperation with SANS.

² The Cyber Preparedness Levels are being developed by The MITRE Corporation.

Levels are different in intent and scope. The CAG intends to aid auditors and provide guidance on assessing the adequacy of security measures employed. The CAG is not designed to provide comprehensive protection against all levels of threats (for example, advanced cyber threats that attack by corrupting the supply chain). Senior executives are the primary audience for the Cyber Preparedness Levels, especially as a tool to assess their company's current security posture and to strategically plan for advancing their security against greater threats. In contrast to the CAG, the Cyber Preparedness Levels activity does not include a means of assessing the adequacy of measures currently in place, as it is intended for use as a strategic planning vehicle, not a compliance vehicle.

We believe that CAG and Cyber Preparedness Levels are excellent examples of how joint private and government work can result in security guidance that is beneficial to both the government and private sector.

In summary, the private sector will need guidance for implementing security controls in a staged manner and to understand how defensive tools and techniques can counter increasing levels of cyber threats. We believe the enhancement of information sharing and visualization from government to industry is a key motivator for greater industry engagement in the pursuit of advanced standards against cyber threats.

Affect of Standards on Procurement and Acquisition Policies

Procurement and acquisition policies need to be modified to reflect certain practices to address high-end or sophisticated cyber threats. For example, the Federal Acquisition Regulation (FAR) addresses requirements for counterfeit commercial products and supply chain protection. The Department of Defense (DoD) also released a memorandum concerning supply chain protection.

Procurement and acquisition policies affected by particular cyber defenses include:

- Development of policies and guidance relating to supply chain protection. Measures may include:

- Import/Export controls.
- Supplier background checks and approvals.
- Mandate multiple and diverse suppliers in contracts. Prime contractors should employ diversity of suppliers to avoid single points of failure or exploitation.
- Minimizing time between order and delivery.
- Trusted shipping (distribution) of critical components to include physical protection and continuous accountability, to protect against supply chain attacks.
- Selective removal or cutouts of critical components prior to shipping.
- Re-implementation of critical components without commercial off-the-shelf (COTS). The most critical custom integrated circuits could be fabricated at a trusted foundry.
- Performing independent code reviews of COTS software and government-developed software. Issues to address include liability.
- Maximization of open source COTS software use and other system components. This will increase cyber security and reduce exposure to the hidden risks of closed, proprietary COTS source code.
- Modification of COTS software to remove unneeded functionality. This will reduce complexity of COTS software to aid in security review, as well as reducing vulnerabilities that may be inherent in certain modules not necessary for mission execution.
- Development of specialized government off-the-shelf (GOTS) hardware/software integrated with operational systems. GOTS will make an adversary's attack planning more difficult.
- Ensure small and frequent changes to software configurations. Frequent changes to software configurations will complicate attack planning and execution.

The government should play a key role with the private sector on supply chain protection, especially with development and sharing of defensive practices and procurement guidance to address advanced cyber threats.

Recommendations for Question One

Recommendation 1: Solve the “Who’s In Charge?” of Cyber Security in the U.S. Federal Government Question

Create a single leadership position at the White House-level that aligns national cyber security responsibilities with appropriate authorities. Specifically identify one government leader for policy, laws, and alignment of resources.

Our group, nearly unanimously, believes that leadership is the key issue to solve most, if not all, U.S. cyber security issues, problems, and challenges. We believe that progress in any cyber security area cannot occur without proper leadership because roles, missions, and responsibilities overlap and are not sufficiently clear. Without firm leadership, attempts to make real progress will be lost.

By selecting the leader and his/her leadership team now, this administration will send the message that the U.S. Government is serious in taking an active role in cyber security. This message will be clear not only to private sectors, but to the departments and agencies of the federal government, our adversaries, and those who prey off of cyber space.

The selection of the President's cyber security leader is the most important and meaningful signal. The leader must be familiar with the political and government processes and be able to work across the federal government and the private sector to ensure success. While cyber expertise and experience is desirable, greater importance is that the leader be able to work effectively across all branches of government, industry and the private sector.

Recommendation 2: Properly Resource and Empower the President’s Selected Leader and His/her Staff

The government should provide the selected cyber security leader with sufficient resources, including Presidential top

cover and legal authority, to accomplish any cyber security-related task. This leader and his/her staff should maintain budget control of their organization and have a strong partnership with the Office of Management and Budget (OMB). By working with OMB, the cyber security organization can ensure that directives are properly resourced across the government and will have the authority to direct OMB to allocate money in order to gain compliance. Budget authority to direct OMB to move resources to positively affect cyber security is necessary.

Multiple government departments, agencies, and branches of government are affected by and play a role in cyber security, many of which are reluctant to give up authority over the matter. Clarification and efficiency in the area of roles, missions, and responsibilities across multiple organizations will take not just legal and policy empowerment, but Presidential top cover and an knowledgeable staff to leverage relationships and work with all stakeholders to accomplish the mission.

Recommendation 3: Clarify Roles, Missions, and Responsibilities in Critical Infrastructure Protection

By clarifying the roles, mission, and responsibilities of the government agencies involved in CIP, a better private-public partnership in CIP protection will be created.

Recommendation 4: Establish a Stronger Working Relationship between the Private Sector and the U.S. Government

The following are examples for carrying out this recommendation:

- *Incorporate private sector cyber threat scenarios within government cyber-related test beds (e.g., DARPA's Cyber Test Range).* Government cyber-related test beds should reflect private sector operational scenarios, especially to demonstrate how similar threats are detected and deterred, as well as to demonstrate private sector concerns (e.g., exploitation of electric utility control system).
- *Participate with private sector test beds (e.g., National*

Question Two

SCADA Test Bed) to demonstrate detection, deterrence, and response to advanced cyber threats. Private sector test beds should incorporate government-developed defensive tools and techniques to increase national awareness of cyber threats and defenses. Lessons learned and worked examples should be incorporated within the private sector (e.g., electric power sector).

- Partner with private sector on cyber security research & development (R&D). The private sector should partner and benefit from government-funded cyber security R&D. Areas of mutual interest and concern should be pursued by the government and private sector (e.g., defensive platforms and consequence management).
- Assist the private sector with integrating cyber security awareness, education, and outreach programs into their operations. Special emphasis should be on advanced cyber threats and defensive tools and techniques. The private sector should assist the government with development of national cyber security awareness programs.

The government should incentivize private sector investment in the development of commercial cyber security products, as well as the rapid deployment of more secure commercial cyber infrastructures. The gap between the government's unique cyber security requirements and the commercial capabilities provided by industry can be narrowed substantially by harnessing the investment power of the free market. This will increase the efficiency and efficacy of the direct government research and development investment.

Recommendation 5: Set and Develop Minimum Standards for Cyber Defense

The improvement of designs, architectures, technologies, and tools are also imperative to building a strong cyber defense that is capable of defending against advanced cyber threats. The offense has a substantial technical advantage. For strong cyber defense, creative and game changing technical approaches and standards are needed.

The common standards should assist private sector

organizations with understanding different cyber threats. These standards should also determine what level of cyber defense they may want to use for a particular system, organization or network. Common standards would also enable private sector organizations to define and assess their degree or level of cyber preparedness. This should be part of an overall strategy to ensure that critical infrastructure applications (e.g., electric, financial) can survive a cyber attack with minimal loss of critical functions. The government should leverage private sector associations as a means to gain consensus on cyber defense standards. Additional information on cyber defense is described further under minimum standards.

Recommendation 6: Develop a National Cyber Recovery Plan

The National Cyber Recovery Plan should address a plan of action for national response to a large-scale cyber attack. A plan is critical due to national reliance on the digital infrastructure, especially with supporting the President's initiatives (e.g., health care, smart grid, and FAA Next Generation). Exercises and simulations should be developed to periodically test elements of the national cyber recovery plan.

Recommendation 7: More Effective Information Sharing and Situational Awareness Sharing Between Network Owners, Operators, and the U.S. Government

Improvements to situational awareness for evolving and changing cyber threats include:

- Sharing threat data, with special emphasis on advanced cyber threats and attacks from nation-states.
- Assessing how the private sector can share a common operational picture of a threat environment with government.
- Incorporating private sector inputs with the development of a common definition of "attack" and norms of behavior.

We must share examples of how organizations detected, deterred, and reacted to advanced cyber attacks. The government should share and help train resources to perform

continuous monitoring and assessment of private sector cyber defenses (e.g., security controls). Sample defensive tools and techniques should be shared, like the sharing of national resources for red and blue team testing.

Recommendation 8: Attribution and Analytics

In order to deter, enforce, and defend, the government and private sector need to work together to fund technologic innovation in the ability to do advanced, real time analytics and processing to achieve attribution. For success in "driving analytics" to achieve attribution, improved information sharing and data access are essential. Additionally, the government and private sector must eliminate or resolve legal and policy impediments to accessing and sharing data.

The government should build and promote multiple virtual communities of interest around cyber issues. Such network-connected communities are now firmly established as responsive and efficient structures for innovation and collaboration by analysts. While there will always be a need for classification and compartmented information, the U.S. should strive to maximize the connectivity of the various cyber security communities of interest.

Much of the success of the current Internet architecture stems from the fact that the architecture ensures there is a unique, authoritative root.

- How would the security and stability of the Internet be affected if the single, authoritative root were to be replaced by a multiple root structure?
- What would be the economic and technical consequences of a multiple root structure?
- What, if any, influences do you see that may:
 - Move the Internet in the direction of greater fragmentation; or
 - Help to preserve and maintain a single, interoperable Internet?
- What are the implications of these forces?

Background

The Internet Assigned Numbers Authority (IANA) is the entity that oversees a variety of critical Internet technical management functions. Pursuant to a contract with the U.S. Department of Commerce, the Internet Corporation for Assigned Names and Numbers (ICANN) executes the IANA responsibility as it pertains to verification of change requests. ICANN is currently a California non-profit corporation. In the context of the Domain Name System (DNS), ICANN maintains the root zone file³, which is propagated to the 13 DNS root server operators for subsequent redistribution to the global Internet. This function is absolutely essential to the smooth

³ The root zone file is essentially an official list of IP addresses for all root servers, and for authoritative name servers for all Top Level Domains (TLDs). It is therefore a very small but critically important file. Generic top-level domains (gTLDs) and country-code top-level domains (ccTLDs) are two of the categories of TLDs.

operation of the global Internet. ICANN's obligations include: (1) maintenance of agreements with all generic top-level domains (gTLD) and most country code top-level domain (ccTLD) operators; (2) accreditation of gTLD registrars; and (3) evaluation of proposed changes and resolution of disputes regarding critical service performed by the Regional Internet Registries, who coordinate through ICANN. Typically, disputes relate to the allocation of Internet Protocol (IP) addresses and Autonomous System (AS) numbers critical for global Internet routing through the Border Gateway Protocol (BGP) protocol. Both BGP and DNS are critical, interdependent elements of the Internet infrastructure. Because of this interdependence, any security issues for BGP or DNS must be addressed jointly.

BGP is the sole protocol for interconnection of otherwise autonomous IP networks (such as Network Service Providers, enterprise, public, and government) that form the global Internet. At present, BGP has very significant security and integrity vulnerabilities, similar to the global DNS services. Specifically, due to original design limitations of this protocol, BGP is susceptible to attacks that modify, delete, forge, or replay data, any of which has the potential to disrupt overall network routing behavior. However, unlike secure DNS (DNSSEC), whose deployment is expected to expand in the future, there is no secure version of BGP ready for near-term deployment.

In summary, current operation of the global DNS and BGP infrastructures suffer from two critical issues that, to a certain extent, are due to insufficient leadership and authority:

- Lack of adequate security
- Lack of effective monitoring

We note that various deployed alternative root servers – not associated with ICANN-approved TLDs – in theory, could replace ICANN-approved root servers. To date, none of these alternative roots has achieved much success, as most users prefer the smooth operations under the status quo, thus accepting the default ICANN zone file. However, if alternate roots gained in popularity, there is potential that the Internet could be fractioned and lead to impediments in global commerce and telecommunication networks.

Discussion

There are currently 13 officially recognized root DNS servers operated by 12 root server operators (see list at <http://www.root-servers.org>). Based on historical precedent and the high level of trust developed between the root server operators, it is highly unlikely that a new, officially recognized, root server operator would be appointed. If a new one were appointed, because of the high degree of trust involved in the root server operator community, a new root server operator based in a country that may be hostile to the interests of maintaining the status quo in terms of stability and security seems unlikely. However, political pressures, possibly coming from the United Nations, the International Telecommunications Union, or individual countries, could seek to revisit the status quo, promoting assumptions and scenarios designed to break the trust level developed over more than a decade on management of critical Internet resources.

If management of the DNS roots was decentralized (beyond a prudent and practical level), the potential impact could include catastrophic security consequences felt globally for the operation of the Internet. Compromise of the roots has always been a primary concern of security researchers. Decentralization of management would also increase the risk of compromise, adding a significant increase in uncertainty for the resilience of a digital economy.

Due to its inherent design, the DNS infrastructure is susceptible to various types of cyber attacks. The primary types of cyber attacks include:

- *Eavesdropping on DNS queries:* Information obtained from this eavesdropping would provide information on active hosts (e.g., .mil systems); however, this information may have minimal value (for network reconnaissance) and could be easily obtained through other means.
- *Executing man-in-the-middle attacks by intercepting queries and redirecting traffic to other sites under their control:* In most cases, the redirection can be easily detected; however, in some cases, such as with email,

any redirection, interception, and reforwarding may go unnoticed by the user.

- *Disrupting the operations of a DNS server:* With the use of mirrored root servers, only local or regional users that normally depend on the affected server(s) would experience any degradation of performance. For root servers that are not currently mirrored, the impact of disruptions against these non-mirrored root servers would be felt globally.
- *Distributed Denial of Service Attacks:* DDoS attacks have severely degraded the DNS in the past. As the sizes and power of botnets continue to grow, the potential for attack on particular root servers remains even though most root servers have employed techniques to distribute the zone widely to other servers.
- *Maintaining the reliability of the IANA oversight:* The current IANA oversight has ensured a successful and smooth operation of the Internet. Any changes risk upsetting the current secure, resilient, and reliable operations. Additionally, the current oversight process is understood by all participants and is generally agreed upon. Changes to the current structure could create unnecessary instability due to uncertainty as entities reach agreement on a new operating model.

These and other cyber attack vectors are not unique to potential adversaries with access to a root server—these attacks are easily and successfully executed regardless of whether the adversary has access to a root server or not. With physical access to a mirrored root server, an adversary could gain access to information stored on the server; however, the vast majority of the information stored on the server is not considered particularly sensitive and is openly available through other channels. At worst, the adversary could obtain a verification key currently used by the root server operators to authenticate data transfers from a master server. This verification key would only allow an attacker to obtain and verify root zone information, which is readily available through other channels. Therefore, aside from any operational disruption, the physical compromise of a mirrored root server has minimal, if any impact.

Based on these circumstances, possession of a mirrored root server by an adversary does not increase the existing level of risk to countries' national security with respect to the DNS infrastructure. The vulnerabilities and impacts related to cyber or physical attacks against the DNS infrastructure remain the same. However, the U.S. and other countries can mitigate some of the DNS-related cyber vulnerabilities through the use of DNSSEC extensions or other key-based authentication mechanisms. Compromise of an actual root has always been a primary concern, and decentralization of the management of this infrastructure would certainly increase the risk of compromise.

DNS Security Issues

DNSSEC protects the Internet from certain attacks, such as DNS cache poisoning. It does this through a set of extensions to DNS that provide: a) origin authentication of DNS data, b) data integrity, and c) authenticated denial of existence.

As of this writing, there is a notable push towards DNSSEC deployment from many DNS server operators, certain ccTLD registries, and some other institutions. With DNSSEC comes the responsibility of an organization, institution, or government to sign the root zone file and appropriately protect the validity of this key. There are many views, and several discussions, on what, or who, should sign the root zone file. Many governments made statements against other governments holding the root zone keys, raising trust as an issue. Neither ICANN nor the U.S. Government has taken the responsibility of signing the vast majority of root zone files such as .com and .net. This leaves over 97% of existing DNSSEC zones isolated and unverifiable as of an October 2008 survey.⁴

ICANN's ambivalence towards zone file authentication for DNSSEC has the following origins:

- A lack of clarity resulted from the U.S. Government interagency decision-making process regarding the desired scope and speed of DNSSEC deployment. The National Telecommunications and Information Administration (NTIA), an agency within the Department

⁴ Quantifying the Operational Status of DNSSEC Deployment. (<http://iri.cs.ucla.edu/papers/imc71-osterweil.pdf>).

Question Three

Our lifestyle is based upon a digital infrastructure that is privately and globally operated.

- How do we get to a public/private partnership and action plan that will build protection and security in – and enable information sharing to better understand when it is under a local or global attack (warning)?
- What is the model public/private relationship?
- Who and how will oversight be conducted in the IC and national security community?
- How would you provide common situational awareness?

Background

Today's World Wide Web and the cyber space to which it has given rise is, for all practical purposes, an open operating environment. Despite its evident risks, that "openness" is believed to be a source of the power of the Web to serve as an engine of social, economic, political, and cultural development on a global scale.

Nonetheless, there is an increasing demand among users for increased levels of security, so long as its provision does not pose, or will not be used to create, undue risk to the ease of operating on the Web or pose a threat to lawful public and private interests.

Public and private sector opinion on the matter has evolved over time to the point of seeking a partnership to regulate activities in cyber space.

The private sector conducts its business on the network. Consequently, our national and international economy is

dependent on network reliability and requires the integrity of the information sent and received. Threats posed to intellectual or other forms of property and to the safe functioning of public infrastructure (industrial, electrical, financial) are real and growing. At the same time, governments at all levels have become heavily reliant on the Web to perform basic functions, provide constituent services, and conduct classic national security functions.

Hence, while private interests and concerns animate the desire to increase Web security, those concerns and interests are not mutually exclusive of national security. That is, activity and operations in cyber space affect not only the daily conduct of business (personal, professional, public and private), but the security of the nation as well.

Because the interests of the public and private sectors are intertwined, public authorities need to engage and accommodate private entities in setting the terms and conditions of the creation of a secure framework for the Web. In short, there is a need for a "public-private relationship" to provide security on the web.

Discussion

Americans are accustomed to such partnerships. For example, Americans are at the heart of partnerships ranging from school boards to regulatory arrangements for utilities. Partnerships form the basis of such organizations as the Civil Air Patrol and local Neighborhood Watches. They can have their origin in a charter, frequently grounded in legislation. Those charters give rise to the creation of regulatory and enforcement organizations, often overseen and sometimes governed by private citizens acting in the interests of the public good. These approaches work best when there is a definable public interest in ensuring that private conduct is not injurious to the public at large, and when private interests recognize the need for legally constituted public authorities to protect individuals in the pursuit of their interests.

An effort to establish such a relationship is not new to cyber space; however, previous attempts at forging a public-private partnership have been sub-optimized, focused less on a

of Commerce, is responsible for leading this process. It is important to note that E-GOV, as part of the Trusted Internet Connection (TIC) initiative, did require and place a timeline on executive branch department and agency adoption of DNSSEC.

- There are substantial geopolitical pressures on ICANN from other major sovereign governments. For example, the operators of the Russian ccTLD registry have publicly stated that the "Russian government will never permit the U.S. Government to authenticate their registries"⁵. Similar difficulties exist with China and other countries.

Such geopolitical forces may lead to the breakdown of the DNS root system into several separately maintained, but plausibly coexisting root zones, and the corresponding root server operators. This would greatly complicate deployment of DNSSEC, and may completely derail its adoption, as multiple roots imply multiple manually configured trust anchors. The Internet Architecture Board spoke out strongly against these alternate roots in "Request for Comments" 2826 (RFC 2826), "IAB Technical Comment on the Unique DNS Root;" however, the basic concerns include:

- Potential significant interoperability and compatibility issues due to increased complexity of federated governance structure
- Significant stability issues due to inconsistent DNS queries across locations

The economic and technical consequences of a multiple root structure could cause the DNS solution to be more expensive, technically more complex due to additional interfaces and management software required, produce the inability to ensure end-to-end security of traffic, and generate potential routing issues resulting from decentralized management.

While ICANN currently controls the root zone, this control consists only of the ability to edit a single file. It is up to the rest of the DNS operators, including the root operators, to make use of this file and propagate the information contained within. There is no mechanism to guarantee operator

⁵ Global DNS Security, Stability, and Resiliency Symposium, February 3 – 4, 2009, Atlanta, Georgia.

compliance, and very little, if any, monitoring of their behavior. Such issues take on a greater sense of urgency when considering the recent attacks against DNS implementations, and more general attacks on Internet routing (BGP) itself.

Recommendations for Question Two

Recommendation 1: Empower NCS and U.S. CERT

Establish the function within the Department of Homeland Security's National Communications System (NCS) and U.S.-CERT to operate, maintain and secure key gTLD's. This includes .mil and .gov domains, complete with a DNS cache, dormant back up, functional rule listed and bastioned for U.S. use only. Working in partnership with the backbone service providers, a contract should be established with these entities to provide a reserve DNS capability similar in concept to the Civilian Reserve Air Fleet (CRAF). These systems would remain passive, e.g. on dark fiber, or some other method, until directed to execute by pre-established conditions or authorization from the US-CERT and NCS.

Recommendation 2: Establish and Enforce an Aggressive Schedule to Move DNSSEC Deployment Forward

Establish a U.S. authoritative working group with a timeline to resolve the U.S. approach to ensure DNSSEC moves forward in a timely manner. This would likely be a government and industry cooperative body that would also need to take into account any global implications of implementing DNSSEC.

Recommendation 3: Address the Multilingual and Multicultural Environment of the Internet

The U.S. should respond to, and support, international demands for ICANN to address the multilingual and multicultural environment of the Internet, and prioritize the development of IdN solutions.

Recommendation 4: Work Internationally to Preserve Current Internet Governance System

The U.S. Government should work with the international community to preserve the current system with respect to the Internet Governance.

comprehensive approach than in adjusting the regulatory environment in a piece meal fashion.

The following are thoughts and recommendations for approaching the creation of, what might be called a “regulatory environment,” that depends on and embodies a public and private partnership to provide for cyber security.

Assumptions

The forgoing suggestions for use of a regulatory environment in building a public-private partnership is rooted in the following set of assumptions:

- The network that supports the World Wide Web is principally owned and operated by the private sector.
- The private sector shares a common sense of concern with the government about the threat.
- There is a need to find a public role in securing both the network and operations on it so that the interests of the private sector are not adversely impacted and privacy concerns are accounted.
- Operations and activities on the network frequently entail interactions among private and public, national and foreign interests.
- The U.S. Government seeks a policy, statutory, regulatory, and operational framework that will evolve to meet U.S. needs.
- There is a commitment by the U.S. Government to draw on private sector advice and use public and private sector experience.
- Cyber space knows no borders; solutions needed must travel well, and quickly adapt to meet changing threats and technology.

Framework Features

The framework for a partnership might have, at a minimum, the following features:

- Based in statute including sanctions for violations.
- Encourages the continued evolution of cyber networks, operations, technologies, and uses.

- Sets security standards for networks and operations.
- Incentivizes private sector behavior consonant with standards.
- Allows for identification of anomalous behavior.
- Provides shared “situational awareness.”
- Defines U.S. Government and private sector roles in incident response, investigation, and remediation to include enforcement of standards and deterrence of destructive behavior.
- Encourages continual innovation and growth.

Regulatory Examples for Consideration

There are examples of regulatory entities that capture some of these features. A fuller consideration might yield others whose features better suit the cyber model. The purpose of the listing below is to provide existing examples that might be mined for elements of a partnership on cyber space.

- *Public Utility Commissions (PUC)*. PUCs are rooted in statute; focused on assuring that public and private needs are served by private providers of essential means for life—power, water; gas. Some PUC features may be unattractive, e.g., their authorities to create rate structures that allow for reasonable profit and growth.
- *Federal Aviation Administration (FAA)*. A feature of interest for cyber space is that the FAA regulates the use of public airspace by private users, individuals as well as corporations. The FAA establishes rules of the road. It provides for management of traffic and has responsibilities relative to the investigation of anomalous behavior (e.g., a crash). The FAA can impose sanctions and directives in support of its charter and in response to anomalous behavior.
- *National Weather Service*. The National Weather Service provides weather reports by monitoring all “activity” in the environment and provides situational awareness and warning universally. Its value is very high even though it has no capacity to change the weather nor is it responsible for any damage caused following its warning.

- *National Geological Survey*. The National Geological Survey is not responsible for topography, but is responsible for the accurate portrayal in maps to guide a wide range of public and private activity.
- *United States Coast Guard (USCG)*. USCG is not a public-private partnership, but does have a regulatory function related to the enforcement of defined behavior on the nation’s waterways and on the high seas. It operates in a civil agency, yet can be “mobilized” in support of national security operations on the basis of agreed terms and conditions.
- *President’s Intelligence Advisory Board (PIAB)*. PIAB is composed of private, non-partisan, citizens that advise the President on the quality of U.S. foreign intelligence collection. A similar organization that oversees, but is not part of the regulatory structure might provide the kind of “final oversight” to assist in the continued evolution of the structures and practices, monitor the threat environment, advise on legislation, etc. This might be a way to ensure a forum for resolving inevitable tensions between national security and other interests in the provision of security on the network and the Web.

International Consideration

Because cyber space is not solely a domestic concern, a corresponding international regulatory model should be identified:

- *International Civil Aviation Organization (ICAO)*. ICAO is the result of a UN international convention; it sets global flight standards yet it presumes national enforcement to include denial of airspace access to non-compliant airspace users. Private participation is via national governments and private airline transportation associations that engage ICAO, and other such international transportation bodies, to help write policies, etc.

Regulatory Conduct

How might a regulatory arrangement function? To assure public confidence at home and abroad, it would require transparency in:

- Government’s interest in and actions in cyber space through its relationships with private sector firms.
- Private sector’s capacity and ability to protect customer interests relative to government demand for access, etc.
- The understanding of the threat by the public via education and building of trust.

The regulatory environment would be inclusive of, and require deep public-private partnership to ensure mutual concerns related to security measures for:

- Hardware
- Software
- Process/Protocols
- Standards
- Enforcement
- Assessments

The objective of a regulatory partnership is to describe an environment that defines broadly and identifies specifically anomalous behaviors:

- Conforming behaviors unaffected.
- On a national level, non-conforming behavior subject to statutory-based inspection, apprehension, investigation, detention and, if necessary, enforcement action.
- With respect to non-conforming behavior, any framework would need to set thresholds where anomalous behavior exceeds the capacity of civil authorities to contain or deter. For that reason, the U.S.CG (noted above) is an interesting example. Most of its work is “civil” in character, however, it can easily and seamlessly incorporate into the national security apparatus to conduct military operations.

Irrespective of the framework chosen, such a threshold will need to be set and some broadly accepted agency charged with defending, deterring, and retaliating against behavior that threatens the national interest.

Recommendations for Question Three

Recommendation 1: Follow a Sequence for Action

- Define the nature of the public and private partnership.
- Identify the purpose of the regulation and the expected result.
- Create the oversight and enforcement mechanism consistent with the two above.

Recommendation 2: Build Upon Existing Models

The more the U.S. Government can use existing models—even if radically revised and integrated in new ways—the more easily it might explain its purpose, intent, and expected outcome. One such model is the DHS & DoD program established to strengthen the cyber security of the Defense Industrial Base (DIB). This program shares sensitive cyber threat information between the federal government and defense contractors via the Defense Collaborative Information Sharing Element (DCISE) at the DoD Cyber Crime Center (DC3). Via the DIBNet, the DCISE has begun to share classified cyber threat information with industry. This fledgling effort shows potential that DHS and DC3 are now exploring expansion of this model to other critical infrastructures. These efforts should be fully supported.

Recommendation 3: Focus U.S. Government Intervention

Focus U.S. Government intervention against behaviors defined through a transparent public/private dialogue that might ease privacy concerns.

Recommendation 4: Build a Public/Private Relationship that is a Complete Model

Both houses of Congress and the Executive Branch need coordinated action and possibly new joint approaches to this issue. Encourage individual members of Congress to lead interaction with constituents to educate, seek public guidance, and be accountable. Encourage Congress to review whether they are optimally organized for action and make necessary changes. Fully engage at state and local

levels for total approach. Educate at the right levels on the threat and nature of technology.

Recommendation 5: Implement Common Recommendations from Multiple Sources

Encourage the Executive Branch to implement the common set of recommendations that have come from CSIS, SANS, BENS, and the GAO, among others. Adopt suggestions that apply across sectors (industry, FFRDCs, government studies, academia) as these share broad public appeal.

Recommendation 6: Fund Efforts for Situational Awareness and Information Sharing

Increase funding to support situational awareness in government centers and information sharing. Where the government funds multiple efforts for an area, and supports different ideas, consensus eventually grows and the best ideas and efforts emerge as standards. By investing heavily in cyber situational awareness and collaboration, the U.S. Government will ensure some of these efforts develop into valuable programs.

Recommendation 7: Educate and Inform Citizens

There are examples in other areas where the Federal government took action to inform on threats and drive awareness. Consider the example of the Cold War yearly series of educational reports titled “Soviet Military Power.” This easy-to-read, but accurate, representation of the threat helped raise awareness and collective action.

Recommendation 8: Focus on Anomalous Behavior Internationally

With respect to the international dimension, focus on anomalous behavior rather than control of the network and operations on it might be more acceptable to foreign, state, and non-state entities.

We believe the actions above, to include moving out on GAO recommendations, will result in enhanced cyber security, functionality of the Internet, job creation, and a more viable economy.

Conclusion

INSA is highly supportive of the presidentially commissioned task to conduct a comprehensive cyber security study and hopes the recommendations in this paper will be complimentary to the effort. As mentioned at the beginning of this report, providing comprehensive cyber security in today’s world is a difficult technical problem. The government must continue to invest in technical improvements to the science of cyber assurance. New policies and procedures are important but are predicated upon continuing improvements in the technical capabilities of government and industry to defend their assets.

The INSA team acknowledges that implementation of any recommendation is only a beginning and that careful nurturing of the progress and process is necessary for long-

term success. While the recommendations offered in this report have provided industry’s perspectives for crafting new and improved cyber assurance policies, INSA recognizes that long-term change will only occur when both the government and the private sector engage each other in meaningful dialog and discourse. The importance of a public/private partnership to address the many technical and policy issues facing our nation in this critical area cannot be understated.

With our private sector partners, INSA stands ready to assist and support the government implementation of the recommendations resulting from the 60-day review of the plans, programs, and activities underway that address issues related to U.S. and global information and communications infrastructure and capabilities.

Appendix 1

About INSA

The Intelligence and National Security Alliance is a not-for-profit, non-partisan, professional association created to improve our nation's security. As a unique forum, where the once-independent efforts of intelligence professionals, private sector leaders and academic experts can come together, INSA identifies critical issues facing our nation in the decades to come. Through symposia, white papers, and debate, INSA's members are laying the intellectual foundation to build the Intelligence and National Security Communities of the 21st century. Through education, advocacy, and open programs, INSA is working to inform the broader public and inspire the workforce from which the leaders of the next generation will rise.

Appendix 2

Contributors

Chairman

Lou Von Thaeer

Question Leads

Steve Cambone

Rob Pate

John Russack

Contributors

Nadia Short

Scott Dratch

Scott Aken

Greg Astfalk

Zal Azmi

Fred Brott

Lorraine Castro

Jim Crowley

Bob Farrell

Barbara Fast

Dennis Gilbert

Bob Giesler

Tom Goodman

Cristin Goodwin Flynn

Bob Gourley

Dan Hall

Vince Jarvie

Jose Jimenez

Kevin Kelly

Michael Kushin

Bob Landgraf

Joe Mazzafro

Gary McAlum

David McCue

Marcus McInnis

Brian McKenney

Linda Meeks

Billy O'Brien

Marie O'Neill Sciarrone

Marilyn Quagliotti

J.R. Reagan

Dave Rose

Mark Schiller

Andy Singer

Mary Sturtevant

Almaz Tekle

Mel Tuckfield

Ann Ward

Jennifer Warren

INSA

Frank Blanco

Jarrold Chlapowski

Jared Gruber

Ellen McCarthy

Appendix 3

Contributor Biographies

Lou Von Thaer

Corporate Vice President, General Dynamics and President, General Dynamics Advanced Information Systems

As president of General Dynamics Advanced Information Systems, Mr. Von Thaer leads a diverse organization of 8,000 professionals that provides end-to-end solutions in systems integration, development, and operations support to customers in the intelligence, maritime, space, and homeland communities. Prior to becoming president, Mr. Von Thaer served in a variety of senior management positions, including senior vice president of operations where he led the integration of the Veridian and DSR acquisitions. Mr. Von Thaer joined General Dynamics as vice president of engineering and chief technical officer after the acquisition of his previous employer, the Advanced Technology Systems division of Lucent Technologies, in 1997. Mr. Von Thaer worked at Lucent and its predecessor, AT&T Bell Laboratories, since 1983.

Mr. Von Thaer holds a bachelor's degree in electrical engineering from Kansas State University and a master's degree in electrical engineering from Rutgers University. He serves on the board of the Intelligence and National Security Alliance and the Engineering Advisory Council for Kansas State University.

Stephen A. Cambone

Executive Vice President, Strategic Development, QinetiQ North America

As executive vice president for strategic development of QinetiQ North America, Mr. Cambone leads the company's strategic planning process and oversees assessments of investment in research and development, technology and development, and the pursuit of new business opportunities. Mr. Cambone also participates in the evaluation of mergers and acquisitions and heads the QinetiQ North America Advisory Board. He previously served in the DoD, during which time President Bush nominated him twice for senior positions, which were then confirmed by the United States Senate. Among other distinctions, he served as first under the Secretary of Defense for Intelligence.

Mr. Cambone received his Master of Science and Doctor of Science degrees in Political Science from Claremont Graduate School and his Bachelor of Science degree in Political Science from Catholic University.

Robert Pate

Chief Security Officer, Renesys

As the chief security officer, Rob Pate is responsible for Renesys' internet data network security services and solutions. Mr. Pate previously served as vice president for cyber security and privacy at McNeil Technologies, deputy director of outreach and awareness at the National Cyber Security Division (NCSD) for DHS, and director of focused operations with the US-CERT. Mr. Pate founded the Government Forum of Incident Response and Security Teams (GFIRST) and led the US-CERT situational awareness program. Mr. Pate came to the DHS from an operational environment where he was the Director of an Incident Response Team for the largest federal civilian agency and the largest healthcare provider in the world.

Mr. Pate earned a Bachelor of Arts in mathematics from the University of North Carolina at Chapel, took graduate work at Johns Hopkins and Stanford Universities, and completed the Senior Executive Leadership Program at Georgetown University. In 2006, he was selected as a "Federal 100" award winner for his contributions to government information technology.

John Russack

Director, Intelligence Community Strategies, Northrop Grumman Corporation

Mr. Russack joined Northrop Grumman in July 2007. Previously, he served in a variety of senior government positions, including the CIA's Senior Intelligence Service on the Director of National Intelligence's staff and on the then Director of Central Intelligence's staff. He also served as the Director of the Department of Energy's Office of Intelligence and as a senior DCI detailee to the Transition Planning Office of the Department of Homeland Security. Previously, he was a career U.S. Navy Surface Warfare Officer and commanded two U.S. Navy warships.

He is a graduate of the National War College, and attended senior U.S. government education at the Maxwell School at Syracuse University and John's Hopkins University's School of Advanced International Studies. Additionally, he is a graduate of the DNI's Intelligence Fellows Program and the recipient of the Director of Central Intelligence's Medal.

Appendix 4

Additional Questions for Studies

What other questions should the National Security Council and Melissa Hathaway ask in order to get the best information available to better focus the Nation's Cyber Security Initiatives?

- How can Government best address overcoming the lack of trust by both the private sector and the general public toward their ability to handle the cyber threat?
- Recognizing the importance of partnership, what is the private sector willing to share with the Government regarding their cyber threat?
- How should the Government engage (and partner with) the State and Local governments in the fight against the cyber threat?
- How should the Government perform the evangelist role in rolling out its cyber security initiative (much like it did with the Y2K initiative)?
- Who should have the responsibility for providing end-to-end cyber security for the Nation?
- Recognizing that the cyber threat is truly global, how should the Government partner with other nations to ensure cyber security?
- Should the Government consider putting into place a National Cyber Defense Education Act?

INSA Industry Task Force





INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Ballston Metro Center Office Towers
901 North Stuart Street, Suite 205
Arlington, VA 22203
Phone (703) 224-INSA
Fax (703) 224-4681