TechAmerica
WHERE THE FUTURE BEGINS
THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

TechAmerica Response to 60-Day Cyber Security Review
Melissa Hathaway
The White House
March 2009

On behalf of TechAmerica, we submit this response to the questions posed to industry on March 5 during a briefing on the White House 60-Day Cyber Security Review. Our comments address the government's role in critical infrastructure protection, thresholds for cyber incident reporting, effective public-private partnership, and the relationship between security, prosperity, and innovation. Our interest in the review and the thoughtful input to our response to these important questions reflects the concern that we collectively have for enhancing our overall cyber security posture.

TechAmerica represents a broad cross section of corporate members across the Information and Communications Technology industry. We appreciate the opportunity to provide this submission as part of the White House 60-Day Cyber Security Review.

Q1: What should government's role be in protecting the critical infrastructure from a nation-state attack?

The primary responsibility for protecting the critical infrastructure lies with the critical infrastructure owners and operators themselves. But, because government has a responsibility to its citizens, its primary role should be to assist with and enable an environment for greater prevention and protection measures for both government and industry and, in the case of a nation-state attack, take a leadership role in defense. This requires a commitment to leadership at the highest possible level. In our Cyber Security paper submitted to the incoming Obama Administration, TechAmerica called for the designation of cyber security as a national priority and the appointment of a cyber security advisory in the White House with strategy development and coordination responsibilities. We believe this level of leadership is crucial for making progress.

We offer the following seven areas where government should play such an enabling role. It is important to note that attribution of a cyber attacks is an on-going challenge for both government and industry. Therefore, neither government nor industry protection and response measures should be solely driven by the nature of the attacker, but by the nature and impact of the attack itself and, of course, applicable law.

(1) The government has a specific and valuable role in protecting the critical infrastructure from a nation-state attack by informing the owners and operators of the critical infrastructure about current known and potential threats from nation-state or other malicious actors and, importantly, by engaging with industry representatives about the spectrum of threats and activity that both government and industry are seeing

TechAmerica
601 Pennsylvania Ave. - Suite 600, Washington, DC 20004 ■ Phone: (202) 682-9110 Fax: (202) 682-9111
1401 Wilson Blvd. - Suite 1100, Arlington, Virginia 22209 ■ Phone: (703) 522-5055 Fax: (703) 525-2279

in cyberspace. Despite the existence of information sharing mechanisms, this level of two-way dialogue and collaboration does not exist today due to legal and organizational cultural impediments. For example, government has been reluctant to revise classification practices (including "overclassification" or inability to provide "tear-lines'), and industry is often reluctant to provide its information (for fear of it being leaked, used for purposes beyond cyber security, or used to impose mandates) in order to allow greater sharing of information. In addition, in the IT context, it is important to note that there are many cases in which information residing on one company's network may not be that company's information, but that of a third party (i.e. customer) that cannot be released but may be important for cyber security measures, particularly in the forensic phase. These gaps hamper the ability of both government and industry to prevent and defend against cyber attacks. Optimum engagement requires a framework that enables two-way information sharing about the threats and malicious activity and collaboration on analysis and mitigation efforts, perhaps through the establishment of information sharing agreements, and takes the necessary steps to protect proprietary information that is passed from the private sector.

Finally, government can improve the security clearance process – and processing – so that more industry representatives can work directly with government officials on threat information sharing and analysis on a real-time basis even for the most sensitive information. For example, streamlining the investigation requirements and applicability across agencies would be a significant improvement.

(2) The government can enhance its ability and its engagement with industry to proactively enforce current cyber crime laws and pursue and prosecute actors that are engaging in cyber attacks. The Identity Theft and Restitution Act of 2008 provided greater leverage for prosecutors to bring cybercrime charges, but more could be done to update the legal environment for cyberspace to address concerns about leakage, liability, or regulatory measures. In addition, such updates could enable greater incident reporting, facilitate information sharing between industry and government for more efficient and effective investigation and attribution, and to enhance cross industry-government training on tools and techniques for forensic, protection, and mitigation purposes.

(3) The government can provide appropriate forums in which the collective industry and government representatives can engage on risk assessment and risk mitigation efforts. The National Infrastructure Protection Plan (NIPP) framework provides such a mechanism for the various industry sectors to engage with their government counterparts under the rubric of the Critical Infrastructure Partnership Advisory Council (CIPAC), with certain protections for the information shared in that forum. That framework should be maintained and utilized when necessary and appropriate to allow for additional collaborative measures. In addition, we encourage the USG to sharpen its work within the NIPP framework, utilizing the Sector Coordinating Councils for policy coordination, strategic efforts, and consensus building and leveraging the SCCs' designated operational arm for information sharing and analysis.

(4) The government can use its diplomatic role and leadership to engage in international dialogue, standards-making bodies, and cross-border collaboration efforts to address cyber security as it is a global challenge in which traditional borders do not apply. Now is an opportune time for the U.S. Government (USG) to engage other countries and take a leadership role in the international dialogue on the future of the Internet and its impact on the global economy and global security in consultation and coordination with the private sector. One suggestion for furthering the US diplomatic role would be to create an appropriate

organization with the Department of State to help coordinate and further US cyber security interests in the international community and help develop an international cyber security strategy. As part of an international strategy, the USG needs to find ways to leverage engagements with key allies and the global community as a whole (perhaps at varying degrees, as appropriate) to collaborate on improving situational awareness, analysis, and response, containment, and recovery measures. Current government-to-government efforts could be bolstered by new institutional arrangements or reduction of barriers to international coordination. In addition, the strategy should articulate where in the international community the USG should engage and with what position(s), and the role/efforts of the agencies engaged to ensure a consistent and coordinated approach. Wherever possible and appropriate, the USG should consult and coordinate with the private sector. Also, wherever desirable, the US can utilize examples of best practices or policies developed in other countries.

(5) The government can invest more productively in research and development (R&D) for cyber security needs as a national priority. Government funding to supplement private investment will be crucial to reaching and maintaining the level of cyber R&D needed to make effective change over the long term. To date, the government – particularly at senior levels – is not sufficiently involved in the coordination of R&D efforts across the government, or in relation to the private sector. To be more effective, government and industry need to have an understanding where R&D investment is occurring (i.e. how the commercial marketplace is driving private R&D investment and where government is spending its resources) so that future funds can be directed to address gaps. The government should continue its R&D coordination efforts under the Comprehensive National Cybersecurity Initiative (CNCI) and IT Sector Research and Development Working Group. More broadly, such coordination efforts should be expanded through cross-sector groups to address the cyber R&D needs throughout the critical infrastructure, and a comprehensive cyber security strategy with associated R&D goals will set the tone for industry involvement and lead to more effective use of available funding sources. The strategy should include, but not be limited to, the following efforts:

- Increasing funding to academic institutions for basic research on security innovation, which is critical to keep pace with the evolving threat landscape;
- Ensuring government participation in the processes of international standards-making bodies and, where necessary and feasible, helping to drive generally accepted standards across the globe; and
- Leveraging the existing cyber test facilities to evaluate the impact of changes introduced into the system.

(6) The government can take steps to improve its acquisition process for cyber security objectives. For example, educating and training those who set requirements for IT programs and streamlining requirements across agencies would go a long way to improvements in the process, and the results. However, it is critical that such acquisition processes do not create barriers for the federal government to obtain the best technology available in the marketplace. Further, we should avoid burdensome regulations that may create a disincentive for vendors to invest in security innovation.

(7) The government can provide certain incentives for industry to take additional security and risk mitigation measures. Additional measures could include further corporate investment in their private cyber security infrastructure to develop redundant architectures. Examples of such incentives could include the following:

- Providing a safe harbor (from data breach notification, for example) for organizations that take preventative and protective measures in advance of an incident that would

reduce or eliminate harm to individuals or organizations (such as measures to render data unreadable if accessed by an unauthorized person). Any such safe harbor should be implemented in a technology neutral manner;
- Examining existing public private incentive programs such as the SAFETY Act to create a Cyber Safety Act; potential liability reduction would be afforded to companies who have exercised effective security practices; and
- Examining modifications to the Stafford Act to enable greater government-industry collaboration in times of crisis/incident response.

By virtue of these measures, the government can help build new global "industrial" leadership for the US in cyber security through its strategic approach in each of these areas.

Q2: What do you see as the thresholds of reporting a cyber incident? When does a threat become important enough to report it, i.e. to your boss, your C-suite, your board members? At what point do you inform federal government?

Some companies indicated that they increasingly see the need for and are taking measures to record and track any incident that occurs on their networks in order to be able to assess down-stream damages or impacts. While any one incident may not raise a red flag at its onset, it may plant the seed for a more destructive attack at a later time. The ability to track that over time, correlate seemingly unrelated events, and trace possible patterns and relationships among events is important for forensic and recovery measures.

The information provided on incident reporting practices is based on the aggregation and generalization of data from TechAmerica member companies. Many companies have processes and procedures in place for reporting cyber incidents, with varying protocols depending on the size and nature of the business and, importantly, the breadth and nature of the incident. Many have requirements that include reporting of any incident to their direct leadership and, based on internal severity ratings or a risk assessment on the level of exposure, to the CIO, COO, CPO, and CEO. In some cases, companies do report incidents to the Board of Directors when impact assessment reveals a critical weakness or material damage or exposure. Companies noted the importance of reporting routinely and in near real-time for effective response.

For reporting outside of their own organization, companies take several aspects into consideration. First, if the incident is broad based and would have an impact on the critical infrastructure, many companies in the IT sector report incidents to the Information Technology Information Sharing and Analysis Center (IT-ISAC). If an incident appears to be of a criminal nature, they may report directly to law enforcement agencies, but in some cases that is only when there is a perception that law enforcement will take action (based on level of financial loss, etc.).

Some companies do have threshold requirements for reporting to the USG outside of law enforcement, such as US-CERT, and they make a risk calculation about that report. They balance the need to share information about that attack or vulnerability with others at the earliest possible time against the possibility that the information they share will be leaked. Should the information be leaked too early, for example, it could put the company and users at risk for reputational or operational loss if protective measures are not in place against possible exploitation. In some cases, the question arises about to whom to report and about what.

Greater information about US-CERT and how and what to report would be very helpful for reporting data. In sum, government needs to make reporting easy and palatable for enterprises to report incidents to the government; government needs to be able to protect the confidentiality of information that is shared; and government and industry need to provide synthesized and analyzed information to improve the "feedback loop" that makes the information more valuable and, therefore, actionable. This would all serve to enhance the relationship between US-CERT and private sector companies, thereby improving information sharing and collaboration on an on-going basis. An important concept to keep in mind for cyber incidents is that their level of severity or impact can evolve over the course of an event, so the situation and, therefore, reporting, is dynamic in nature.

In all such incident reporting, whether internally or externally, the process only works when a level of trust has been achieved among relevant parties. Within an organization, trust is more implicit and easier to establish and is, ideally, supported by internal operational policies that map to various legal and regulatory requirements. Establishing trust relationships outside of an organization, particularly between an organization and the government, is more difficult. This trust challenge must overcome cultural and operational barriers. Operationally, the capacity of each department, agency, or organization to deploy appropriately – and similarly – skilled individuals to ensure effective use of resources and collaboration remains fundamental to establishing trust. When the technical experts in one organization to communicate regularly with their professional peers in other organizations it supports trust building and, therefore, greater collaboration.

Finally, many companies have USG entities as customers, or customers that hold personally identifiable information (PII) or other sensitive data for the government. In those cases, companies comply with federal reporting guidelines to advise their designated information security contacts accordingly. The issues around data breach can prove illustrative for reporting thresholds, as follow:

With respect to PII, breach analysis services have evolved and can provide the insight needed to support an agency's response to a possible data breach such as:

- Determining whether or not a breach has caused harm through investigation of the circumstances and an understanding of the data security measures put in place for loss prevention purposes;
- Identifying harm directly attributable to a breach as opposed to pre-existing "environmental" fraud;
- Proactively detecting data breaches within an organization's databases; and
- Pinpointing organized misuse of PII due to a breach, enabling organizations to provide targeted victim remediation, and facilitate law enforcement efforts.

While some government agencies take advantage of these technologies, or are required by law to do so, most do not. As such, the government should consider utilization of commercial best practices that continuously monitor systems for incidents involving loss of PII.

Q3: What changes are needed for an effective framework for the public-private partnership (including an action plan, accountability, shared situational awareness, response, etc.)?

The most important step toward improving the effectiveness of the public-private collaboration would be to provide a reliable and trusted forum for sharing information and collaborative analysis (for situational awareness and a common operating picture) as well as implementing predictable and coordinated incident response and recovery measures. Clarifying the needs and requirements as well as roles and responsibilities in such framework would assist in developing an action plan for concrete steps and benchmarks. The NIPP framework has been set up for this purpose and could serve to provide an effective forum if the impediments to information sharing and collaboration (see response to Q1 above) are addressed.

The government should commit itself to one mechanism for such a framework (such as the NIPP) so there is one set of actions, benchmarks, expectations, etc. (even with appropriate sub-parts vis-à-vis policy and operations, respectively, under one umbrella framework) where industry and government partners can engage. Currently, there are various groups for government-industry consultation and input and general government outreach to industry is ad hoc and uncoordinated across agencies, which causes duplication of effort and disjointed results. This situation could improve with greater coordination, consolidation, and rationalization across the various bodies. The interaction with one such partnership mechanism does not mean that the full range of outreach and engagement with partners across the various stakeholders (e.g. universities, NGOs, municipalities, citizen groups) would be limited, but the partnership efforts with such disciplined action and ability to communicate and collaborate in a trusted environment would reside in one manageable construct.

On specific way in which we can improve the operational partnership specifically is to include industry representatives in the government watch center (i.e. US-CERT) to facilitate on-going, collaborative response and analysis efforts.

It is important to note here that companies that are providing products and services to the government are subject to contractual action plans and accountability mechanisms that should be considered in the context of public-private partnership.

Q4: How do we balance security with prosperity and innovation, including amplifying the needs rather than hindering them?

The relationship between security, prosperity, and innovation should be viewed and leveraged as a synergistic one, rather than a “balanced” one. Cyber security is an important component of prosperity and innovation, particularly in the context of the nation’s digital economy. Should one element ever threaten to come at the expense of another, government and industry leadership should engage immediately to take action that will ensure the continued pursuit of each. Privacy and civil liberties are also crucial to sustaining the trust and confidence in our information infrastructure and electronic commerce. Again, should these ever be threatened, government and industry leadership should engage for addressing those issues appropriately. There are two elements to a successful approach to achieving security, prosperity and innovation.

First, government and industry should engage to develop and then implement a national strategy for cyber security that reflects security, prosperity, and innovation and incorporates related principles.

Second, policy-making through either legislation or regulation should also reflect these three objectives and related principles. This would include ensuring ways to preserve the business models that companies employ today (e.g. COTS products, global supply chain, product development processes) and the flexibility to respond to a rapidly evolving environment while building security in to the processes, rather than imposing overly burdensome and unworkable requirements or creating a patchwork compliance regime.

Any other approach could lead to a situation in which the government is not able to procure the most state-of-the-art products and services to meet its mission(s) either because the cost is too high or the procurement process is too slow to take advantage of the most current technology. Similarly, overly-restrictive measures could hamper the ability for leading US companies to leverage global production opportunities or market growth, thereby hindering overall US economic leadership and weakening US and global security efforts.

In sum, cyber security contributes to the trust and reliability of the critical infrastructure on which productivity and innovation depend, enhances inter-party (and inter-sector) collaboration and innovation, and helps build long- and short-term partnerships that maximize economic value.

Conclusion

Thank you for the opportunity to provide this input into the Administration's cyber security review. We are happy to answer any further questions you may have and look forward to our continued partnership with you on this critically important issue.

The Technology Association of America is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. Representing approximately 1,500 member companies of all sizes from the public and commercial sectors of the economy, it is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). The Technology Association of America was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Association (GEIA). Learn more at www.aeanet.org or www.itaa.org.