1615 H Street, NW
Washington, DC 20062-2000
Tel: 202/463-3100
Fax: 202/463-3177
E-mail: abeauchesne@uschamber.com

U.S. Chamber of Commerce

www.uschamber.com

Ann Beauchesne
Vice President
National Security & Emergency Preparedness Department

March 27, 2009

Ms. Melissa Hathaway
Senior Director for Cyberspace (Acting)
National Security Council
Executive Office of the President
1650 Pennsylvania Avenue, NW
Washington, DC 20504

Dear Ms. Hathaway:

The U.S. Chamber of Commerce ("Chamber"), the world's largest business federation representing over three million businesses and organizations of every size, sector, and region, respectfully submits the following answers to questions which you raised earlier this month at an industry meeting, in which the Chamber participated, as part of the White House's 60-day review of all government plans, programs, and activities underway that address our communications and information infrastructure (i.e., cyberspace).

As you may know, the Chamber is the principal voice of the United States business community and its members take very seriously the threat that cyber attacks have on the economic and national security of the United States. The Chamber commends the White House for its open and consultative approach to conducting the review, and the Chamber offers the following comments in the same spirit of cooperation. Consistent themes expressed by members include the need for a national policy to ensure the protection and resilience of the private sector in the face of cyber attacks; improved information sharing between industry and government; and increased government funding of cyber security research and development (R&D).

1. **What should the federal government's role be in protecting critical infrastructure from cyber attacks from nation-state/non-nation-state actors?**

The federal government should take a number of actions to protect critical infrastructure from cyber attacks from nation-state/non-nation-state actors, including ones which:

- Set a national policy for ensuring protection and resilience of our nation's critical cyber infrastructure and key resources (CI/KR) during crises/emergencies.

- Initiate an education and outreach campaign to raise public awareness of cyber threats and promote cyber security
- Notify sectors/individual businesses if government agencies become aware of efforts by foreign entities or organized crime to launch attacks against United States industry
- Create and exercise a national cyber security preparedness, response, and recovery plan in the event of a large-scale attack

- Address not only physical and information infrastructures but also include critical information protection.
  - Clarify roles, responsibilities, and authorities (e.g., address relationships among the Department of Commerce, Department of Defense, Department of Homeland Security (DHS), and the intelligence community) and the relationship with the private sector, and its roles/responsibilities
  - Provide the organization with the resources and legal authority to effectively execute its mission
  - Increase the effectiveness of government agencies' ability to identify/pursue parties who attack government and/or CI/KR networks

- Improve information sharing between government and the private sector – better "give-and-take" – to protect critical infrastructure and the wider business community. A good model from which to build exists with the information sharing and analysis centers (ISACs). However, utilization of ISACs is not currently consistent across the 18 CI/KR sectors or the wider business community. Both public and non-public sources of data should be leveraged to communicate timely and actionable information to CI/KR components.
  - Share early warning of cyber threats or attacks
  - Provide new and effective methods to "clean up" an infected enterprise or mitigate damage due to intrusions or attacks
  - Provide concrete benefits (e.g., R&D funding, timely notice of threats) from sharing information
  - Develop methods of private-sector information sharing without attribution (Information provided to government by the private sector, which is intended to help counter cyber threats, must not be used against the company providing it by any other government agency.)
  - Enact legislation similar to the SAFETY (Support Anti-terrorism by Fostering Effective Technologies) Act to address risks associated with information sharing by the private sector

- Establish a means to partner with the private sector to drive commercial off-the-shelf (COTS) industry to raise the bar on creating effective cyber security solutions as well as provide R&D funds to help spur COTS leap-ahead efforts.

- Create an incentives program for industry to adopt cyber security practices, including establishment of value propositions/demonstrable return on investment.

- Identify and control all ingress/egress points from the Internet and external networks connecting to government networks.

- Enforce/enact laws that enable swift prosecution of cyber crime and protections for cooperating Internet service providers and other relevant participating private industry.

- Engage in international dialog and lead efforts that promote:
    - A global approach to addressing cyber security
    - International cooperation for prosecution of cyber crime (e.g., Council of Europe Convention on Cybercrime)
    - Information sharing among nations

- Use government acquisitions process to improve security of our nation's infrastructure; protect competitively sensitive information shared from government acquisition reviews. Clarify in government contract requirements:
    - Cyber security expectations
    - Protection of data and privacy (balance)
    - Security standards

2. What are the thresholds at which businesses/organizations report cyber security incidents to government entities like US-Computer Emergency Readiness Team (US-CERT)?

Businesses report cyber security incidents when violations of personally identifiable privacy (PII), federal/state law, or customer contracts occur. However, businesses may not consistently report general cyber security incidents. In certain sectors, a company will likely not report a cyber incident to US-CERT, unless it is beyond the company's ability to resolve on its own. Crisis communication processes being implemented in some sectors, for example, are designed to enable owner/operators to first discuss an incident within the sector to determine the sector impact before reporting it to the government (consistent with the law). Participation in the process includes the cyber security professionals (e.g., information technology (IT) and industrial automation and controls) and physical plant security professionals. In addition, many CI/KR companies have well established relationships with state and local law enforcement agencies. U.S. Chamber members also report cyber incidents to appropriate agencies which compromise:

- Export control data
- Classified government data
- Privacy data
- One percent or more of company revenue

3. **What specific changes are needed to make public-private partnerships more effective and workable? (What measures are necessary to ensure an approach where "action plans" are employed and which businesses/government can effectively measure progress toward a cyberspace that is "assured, reliable, and survivable"?)**

Many changes are needed to make public-private partnerships work more effectively. Some of them include:

- Enabling improved collaboration between government and the private sector – particularly at a time when a weakened economy is forcing many businesses to strictly manage resources and limit costs.

- Building upon existing (regional) partnerships for ideas. For example, since October 2008, the Chamber and DHS have been partnering in four roundtable events across the country – from Boston to San Diego – to increase the level of cyber security awareness by business and to encourage investments in cyber security from an "enterprise" perspective. The Chamber-DHS partnership allows leading experts from the public and private sectors to communicate to the business community the significance of cyber security as a national challenge and to offer some solutions. The Chamber is seeking to build on this partnership in 2009 and beyond. (See enclosed Chamber cyber security regional education and outreach one-page brief.)

- Leveraging existing security standards germane to specific sectors – such as the "CFATS" (Chemical Facilities Anti-Terrorism Standards) program being implemented by certain facilities in the chemical sector – rather than creating new or overlapping requirements or regulations. Private sector input should be an integral part of any regulatory or standards-setting process. A "one-size-fits-all" approach by government and the private sector to achieve a cyberspace that is "assured, reliable, and survivable" is most likely impossible, since each sector is unique.

- Considering risk transfer tools (e.g., insurance) to address corporate risk and creating an environment in which best practices, transparency, and compliance management are the predicates for the provision of insurance.

4. **How can industry and government achieve a national cyber security posture which encourages innovation and economic prosperity?**

Government and industry can pursue several initiatives to increase national cyber security while encouraging innovation and economic prosperity, including initiatives which:

- Fund research in cyber security. Government should fund government-sponsored cyber security R&D for leap-ahead technologies (e.g., by universities and industry).
    - Create a national pool of funds dedicated for cyber security innovation and operate a new civilian advanced research organization similar to the Defense Advanced Research Projects Agency's (DARPA) concept where R&D is linked to specific commercial cyber security needs.

- Consider incentives to help industry meet cyber security standards, thus enhancing the nation's cyber security posture. Make incentives scalable to those businesses which implement the highest standards.

- Use the federal government's procurement power to support commercial markets for secure operating platforms and network services. Make such technology and services available to industry for deployment of critical infrastructure by including stricter/more sophisticated requirements for secure technology in their request for proposals.

In closing, the Chamber would like to express its support for the goals and objectives behind the review of government efforts to protect cyberspace. The Chamber and its members appreciate the willingness of the White House and your team to reach out to the private sector on these issues. The Chamber appreciates having the opportunity to present its views on this matter. The Chamber looks forward to continuing a dialogue with you and government partners on this subject.

Sincerely,

Ann Beauchesne
Vice President
National Security and Emergency Preparedness Department

U.S. CHAMBER OF COMMERCE

U.S. Chamber of Commerce
National Security and Emergency Preparedness Department
Cyber Security Working Group ─ Regional Outreach and Education

In early 2008, the U.S. Chamber of Commerce launched a Cyber Security Working Group to educate its members and influence the cyber security debate. Recent landmark developments – from the Bush Administration's "cyber initiative" to the Center for Strategic and International Studies' cyber commission report to the Obama Administration – have elevated protecting cyberspace both as a policy and political issue. At day's end, effective cyber security practices mean well protected and resilient critical infrastructures which comprise the nation's economic backbone, and they also mean businesses that continue operating effectively, selling goods and services to the marketplace, and employing countless Americans.

Emphasizing an "Enterprise" Approach to Cyber Security
Since October 2008, as an outgrowth of the cyber initiative, the Chamber began partnering with the U.S. Department of Homeland Security (DHS) increase businesses' awareness of, and investments in, cyber security from an "enterprise" perspective. Through its national network of partners, the Chamber has coordinated outreach to business owners and operators as well as incorporated participation from regional, state, and local government security officials.

This public-private partnership stresses the potential consequences of a cyber attack on businesses, and it calls upon the businesses to better integrate cyber security into organizations' enterprise risk management, emergency management, business continuity planning, and cost-benefit decision-making processes. Importantly, the regional roundtables give Chamber members a valuable opportunity to showcase their viewpoints and offer suggested practices for protecting cyberspace. Recent outreach and education initiatives include:

- Oct. 14, 2008 – U.S. Chamber forum on enhancing industry cyber security, featuring DHS Secretary Michael Chertoff and several Chamber members
- Oct. 20, 2008 – U.S. Chamber/New England Council (Boston, MA)
- Feb. 18, 2009 – U.S. Chamber/Bellevue Chamber of Commerce (Bellevue, WA)
- Mar. 26, 2009 – U.S. Chamber/Ann Arbor Area Chamber of Commerce (Ann Arbor, MI)
- Apr. 10, 2009 – U.S. Chamber/San Diego Regional Chamber of Commerce (San Diego, CA)
- May/June 2009 and beyond – TBD