

Incentives- Liability/Safe Harbor **Recommendations**

The Private Sector

1. Continue to refine efforts to establish generally accepted measurement tools to evaluate corporate and individual cyber security based on widely accepted and recognized best practices and/or standards.
2. Develop coherent programs utilizing these measurement tools to establish programs of qualification, compliance and/or certification.
3. Establish third-party designations that identify qualified, certified and/or compliant organizations and making awards ranging from “seals of approval” to designations of excellence (similar to the Baldrige Award).
4. Take advantage of the cyber-risk management programs and services offered by the cyber-insurance industry as a means of providing for business continuity and financial risk management.
5. The Insurance Industry should modify the degree of availability as well as the cost of cyber-risk insurance protection based on the degree that the company exercises cyber-risk best practices.
6. Consider establishing appropriate and lawful programs that seek to use market forces to motivate partner and user organizations to enhance their cyber security programs and practices. Industry leaders, including trade associations and sector coordinators should be encouraged to identify and promote such programs among their respective client base.

The Government

7. Encourage appropriate availability and use of cyber-insurance as a means to protect this nation’s critical assets [This recommendation is discussed “PUBLIC SECTOR ACTION ITEMS TO SUPPORT MARKET BASED INCENTIVE PROGRAM”]
8. Congress and DHS can assist by publicize the positive efforts that are being made by individual corporations to improve cyber security beyond their own corporate walls.
9. Consider legislation providing liability limits and/or safe harbor protections to private sector entities. Specifically, Congress would determine whether or not such legislation would be an appropriate incentive as part of the overall effort to encourage the private sector to adopt and implement effective IT security controls.
10. Investigate “economic incentives” that would reward, for a fixed time period of time, capital investments made by companies when they purchase “certified or

qualified” information security products and services.

11. Enact procedures whereby in cases of a covered cyber-disaster FEMA payments would be modified based on the extent in which best practices (including purchase of cyberinsurance) was executed.

12. Ask CRS, or another appropriate body, to consult with the private sector and prepare an inventory of state and local, national, and international regulatory requirements relating to cyber security.

13. Encourage appropriate availability and use of cyber-insurance as a means to protect this nation’s critical assets.