PITAC CYBER SECURITY SUBCOMMITTEE

JULY 29, 2004

TOWN HALL MEETING ON CYBER SECURITY RESEARCH AND DEVELOPMENT QUESTIONS

Those who are providing oral comments are asked to address one or more of the questions below.

1. What are the greatest threats to Federal cyber infrastructure today? What are the greatest threats to the private sector cyber infrastructure today? How imminent and serious are these threats? On what basis are such threat assessments made?
2. What are the most important capabilities that need to be strengthened to defend against these threats?
3. How can we establish an effective process to assess threats and vulnerabilities on an ongoing basis? How can we better understand the potential consequences of these threats and vulnerabilities? How could we use such assessments to respond meaningfully to these threats and vulnerabilities in a timely manner?
4. What are the biggest obstacles in developing pervasive trustworthiness in the Federal and private sector cyber infrastructure?
5. What are the most essential, the most challenging, and the most promising technical research problems that need to be solved in order to substantially improve the security of the nation's cyber infrastructure?
6. Critical infrastructures are controlled by computing and communications systems. Do these systems have distinctive cyber security issues as compared to other types of computing and communications systems? If so, what are they and what needs to be done to address these issues?
7. What are the key issues involved in infrastructure interdependencies, including the physical security of cyber infrastructure (including telecommunications)?
8. What are the advantages and disadvantages of the open source software model in supporting improved cyber security?
9. How well do the operational practices within organizations manage the risk from cyber security threats? What lessons (both positive and negative) from current practice deserve to be adopted more broadly?
10. Would new data collection or the increased availability of existing data facilitate improved decision-making by those responsible for the day-to-day management of the cyber infrastructure? If so, what kinds of data would be most helpful? Are data standards/metrics needed and, if so, which ones?
11. Is the pool of knowledgeable researchers, developers, and managers in cyber security adequate to protect the nation's cyber infrastructure? If not, how does the pool need to be strengthened?

12. What are the major legal issues that need to be addressed that would promote the development and deployment of cyber security technologies? Such issues may include (but are not limited to) intellectual property and software liability. What can be done to enhance the capabilities of law enforcement to prevent and prosecute cyber space attacks?
13. Where and how should the Federal government invest its cyber security R&D funds? Is the Federal government investing enough in cyber security R&D? Is the allocation for research vs. development optimal?
14. How can public-private partnerships be effective in fostering improved cyber security?
15. Some of the Government's research funding for cyber security is directed towards classified work. To what extent and for what reasons should the Government support classified work?
16. What are the major barriers to technology transfer of Federal cyber security R&D to the commercial sector? How do these barriers differ for work that is performed by the Federal government directly as compared with work that is funded by the Federal government but is performed by others?
17. What are the major barriers to technology transfer from the commercial sector to Federal cyber security R&D activities?
18. To what extent do you believe that market forces can provide sufficient incentive to develop trustworthy systems on a widespread basis?
19. What are the most effective incentives that would encourage the deployment of existing cyber security technologies? How does the existence of a dominant computing platform affect the efficacy of such incentives?
20. How might the coordination of the various cyber security research and development activities within the Federal government be best achieved?