



DEPUTY SECRETARY OF DEFENSE  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

MAY 19 2011

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) Task Force on Cybersecurity and Reliability in a Digital Cloud

You are hereby directed to establish a Task Force to evaluate all aspects of providing reliable, secure, and responsive services for military and intelligence applications using these technologies. Specific purposes of this Task Force include:

- Characterize the operational properties of clouds and virtualized infrastructure, and the quality of service that can be delivered to connected users, paying particular attention to attacks on communication that would destroy or delay delivery of services and information for time-critical uses;
- Consider alternative designs and implementations of these technologies and evaluate their use for varied military and intelligence applications;
  - Discuss options for inter-cloud services and other communications between clouds, especially between clouds that operate at different classification levels, have different authorities, or are operated on behalf of different agencies and organizations;
- Evaluate the vulnerability and risk mitigations of a cloud infrastructure to various attacks, compared to alternative infrastructures;
- Evaluate the vulnerability and risk mitigations of virtualized infrastructure to various attacks, compared to alternative infrastructures;
- Determine how to avoid the danger of concentrating data and computation; for example, suggest how diverse (non-homogeneous) software and hardware can be deployed in the cloud to enhance reliability and security;
- Review and project the consequence of current trends in digital technology on cloud deployments, including social computing;
- Comment on customer practices and modes of interaction with the cloud that might aid in increasing security;
- Make recommendations on what dimensions (pros and cons) of these technologies should be considered to increase reliability and to ensure security as the military and intelligence communities evolve their digital infrastructure;
- Comment on workforce implications (skills, qualifications required, etc.) the Department might expect in transitioning from current environments to cloud implementations;
- Identify research opportunities and estimate the level of investment to achieve results consistent with DoD needs;



OSD 04475-11



- Assess cost/benefit and effectiveness/suitability issues associated with Software as a Service, Platform as a Service, and Infrastructure as a Service, as those technologies apply to both garrison and deployed computing requirements; and
- Identify methods to leverage the rapid innovation and operational maturity being delivered by public cloud providers while maintaining the Department's ability to service its own IT needs effectively and operate at multiple classification levels.

The military and intelligence communities are increasingly articulating a need for information systems that rely upon cloud computing, virtualization, and related technologies. A digital cloud has a richly networked, distributed core of data storage and computational resources that provides shared information and services on demand to individual users located outside the cloud, but connected via a network. Cloud advocates assert that infrastructure incorporating cloud-based technologies and virtualization can deliver both higher reliability and more assured cybersecurity.

Administration support and funding will be provided by the Under Secretary of Defense for Acquisition, Technology, and Logistics. Additional support will be provided by the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), the Director, Operational Test and Evaluation (DOT&E), the Vice Chairman of the Joint Chiefs of Staff, and the Commander, U.S. Cyber Command. All Task Force members, consultants, and supporting personnel will be appointed or designated in accordance with DoD Instruction (DoDI) 5105.04, "Department of Defense Federal Advisory Committee Management Program."

The Task Force will be established and operated in accordance with the provisions of the "Federal Advisory Committee Act" (5 U.S. Code Appendix, as amended), DoDI 5105.04, the DSB Charter, and all applicable laws, policies, and regulations. It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

