RICHARD P. LEE
9471 Harrowhill Lane
Burke, VA 22015-1538

July 26, 2010

Subject: Testimony before the Terrorism, Unconventional Threats and Capabilities subcommittee of the HASC on *Harnessing Small Businesses Innovation for National Security Cyber Needs*

Thank you for inviting me to address the Subcommittee on this topic of increasing importance to the Nation. I approach the challenges of maintaining and sustaining the cybersecurity of our Nation's information resources from a lifetime of exposure to the intersecting demands for rapid, reliable information sharing and protecting the confidentiality, integrity and availability of that information – the three pillars of Information Assurance.

I understand of the focus of the Sub-Committee's hearing is on the challenges and impediments to enabling the Nation's ability to dominate and operate in the emerging cyber space arena, and to taking advantage of American technical know-how. Because the Nation's economy and operational capabilities depend on Internet connections – our ability to manage and respond to crises, our ability to access and share data and information, and our ability to communicate and collaborate – we must not abandon the "battlefield" but must find ways to operate through attack.

A significant challenge facing the Nation, particularly when executing governmental functions, is how to harness the passion, originality and resourcefulness of US innovators. Users, collectively the operational mission elements, are expected to articulate their requirements in technical terms. A problem is that operational elements and technical solutions providers often "talk past" each other – the former trying to describe what is needed in mission language; the latter hearing the need in terms of the products or implementations with which they are familiar. Too often, rather than take a step back to apply holistic systems engineering principles, engineering effort is expended to fix a discovered vulnerability, meet an emergent external threat, or enable tighter control over the user community – countering the "insider threat".

In my opinion, there are three primary areas that impede innovation and the introduction or adoption of novel approaches to cyberspace threats:

A. The acquisition process
B. The Evaluation and Certification Process
C. Financial resources

The acquisition process pulls cyber solution space toward the "big pocket" integrators who can afford the "Bid & Proposal" process funding needed to compete for implementation contracts. In a normal hardware based large system acquisition, the technical proposal is often limited in size, is focused on responding to technical specifications that bound the competitive space, and often "wins" on best value (*i.e.*, cost to implement and sustain.)

Difficult to estimate are potential costs to transition from existing systems implementations to the new. Impossible to estimate is the "lost opportunity" and future costs from only "patching" the architecture with upgrades and incremental fixes. Recall Albert Einstein's statement: "No problem can be solved from the same level of consciousness that created it." (http://www.tc.umn.edu/~burc0050/quotes_einstein.html)

Total Cost of Ownership (TCO) is also difficult to estimate, including the potential impacts on physical plant (space, weight, power, heat dissipation or air conditioning required), manpower, training, and logistics issues. Larger companies experienced in providing solutions to government customers are often better able to navigate the proposal process, describing offerings in language familiar to proposal evaluation teams. An effect may be an inadvertent and unrecognized institutional bias toward a well crafted proposal without appreciation for underlying "sameness" of the technology to current implementations.

The evaluation and certification process is king in the government cyberspace arena. For valid reasons, cyber technology solutions must be known to work, the vulnerabilities to attack, breach, exploitation or failure understood, and *a priori* plans made to mitigate, manage or respond to potential situations in which system functions are in jeopardy. A problem is that there are few practitioners available to evaluate cyber space technical offerings. As a result, technology offerings are required to conform to existing standards and implementations that have been studied, and their vulnerabilities understood. Starting from that point, the evaluators can quickly assess the "correct" implementation of the standards invoked in a solution, can assess how the known vulnerabilities inherent in the standards are mitigated or addressed by the solution, and can accomplish however much "penetration testing" may be called for given the planned environmental use for the solution, *e.g.*, will financial information, secret military information, or other information be processed on the system?

Since the evolution of many of the cyber space standards and protocols were originally developed in an academic environment where trust was assumed between colleagues, mitigating some of the now known vulnerabilities has required layering on manpower intensive procedures, monitoring and internal "fire-breaks" to prevent exploitation of the "insider threat" – the disgruntled or malignant human operator, poorly designed or malfunctioning hardware or software, or poorly trained or inattentive user.

The dilemma facing the evaluation and certification communities are that new often proprietary approaches, innovative implementation of defined standards, or novel

concepts require first understanding the "new" (getting into the innovators' heads), evaluating the concepts, architectures, or proposed implementations for potential vulnerabilities, and then assessing the specific implementations against the just evaluated approach. Without a stated government customer who can define the planned operating environment where the new solution will be used, evaluation of proposed mitigation techniques (*e.g.*, administrative processes, physical access controls, *etc*.) cannot proceed. With limited resources to recruit, train, and maintain trusted evaluation staff, the workload is daunting. A result is a bias to embrace current architectures, approaches, and standards and protocols with known vulnerabilities.

Some people have proposed a "fee for evaluation service" approach in which the innovators can fund the evaluation of their innovative or novel approaches to cyber problems. A problem persists, however, in identifying the planned environment in which the solution will be employed. The resolution of that problem lies in "the Champion" for the solution – the person with sufficient influence and authority to "pull" a novel solution into evaluation. A difficulty for most small business innovators is finding the government official or organization that can perform the role of "Champion," and then gaining an audience to expose the solution. The acquisition process further dissuades this approach to avoid an appearance of competition manipulation.

There are some programs and initiatives pursued by Executive Departments to provide fora for the exposure of innovation to the people with the problems to solve. Two examples include DARPA programs and the Defense Research and Engineering Directorate Joint Capabilities Technology Demonstration Program.

Recommendations:

1. Fund research and development innovation incubation initiatives that formalize linking innovators and "Champions" to accelerate identifying operating environments and promising technologies.

2. Fund expanded evaluation activities to more quickly respond to novel or innovative approaches to cyber solutions.

3. Direct Executive Departments to report on systems engineering activities to examine holistic approaches to cyber challenges. (*E.g.*, how might an emerging computing and communications multi-core hybrid fabric mesh enable defense in depth security services?)