DEPARTMENT OF HOMELAND SECURITY
Office of the Under Secretary for Science & Technology
FY 2008 Report of Closed Meeting of the
Homeland Security Science & Technology Advisory Committee
Under Section 10(d)
Federal Advisory Committee Act

The Homeland Security Science & Technology Advisory Committee (HSSTAC) met in a partially closed session on July 15, 2008 in Arlington, VA. The determination to partially close the meeting was based on the consideration that the briefings and discussions during the meeting would involve classified information sensitive to homeland security. Disclosure of the information discussed could potentially increase the risk to our nation's security due to the identification of vulnerabilities and the potential areas of focus for future research to mitigate our vulnerabilities. All sessions of the meeting were closed to the public pursuant to the provisions of 5 U.S.C. 552b(c) with the exception of the open session on day one.

The objectives of this quarterly meeting were to discuss the last year's Improvised Explosive Device (IED) assessment (IEDs: Coming to America, 29 February 2008); review current committee efforts; and solicit input from attendees on future efforts.

Mr. Norman Polmar, Committee Chairman, welcomed the attendees and explained the HSSTAC, which was established in 2002, met for two years and then went into hibernation for over a year before it was reestablished last July. The committee was asked by the Under Secretary of the Department of Homeland Security (DHS), Directorate of Science & Technology (S&T) to put together an assessment of IED threats in the future. In order to meet this tasking, the committee broke into panels and looked at IEDs coming into the U.S. The methodology for doing this was conducting several interviews and briefings with various organizations, including many British organizations dealing with the IRA and other threats.

The assessment included varying views of what constituted an IED. There are two chains described in the report – the "kill chain," which describes the steps necessary for the execution of the IED attack; and the "response chain," used to related counter-IED (C-IED) activities to the terrorist kill chain. The key to effective C-IED measures is to get to the left of the kill chain, or in other words, try to get to people and the sources of the development of the bomb before it is set off.

The IED assessment that the committee finalized included six major findings:

1. The use of IEDs by terrorists within the United States is a real, agile, and complex threat.
2. Countering IEDs in the domestic environment is significantly different from countering them in combat zones based on different operational environments and policies.
3. DHS S&T does not effectively leverage applicable national counter-IED investments.
4. The current DHS S&T IED program is primarily focused on countering the devices and does not have sufficient emphasis on the human component of the IED threat.
5. DHS S&T does not sufficiently incorporate the requirements of diverse local, regional, and state responders in its planning.

6. DHS research and development (R&D) programs do not effectively support social and economic resilience to IED attack and post-attack restoration, although this role for DHS S&T is limited under the enabling legislation.

Each finding was briefly addressed during the committee meeting. For Findings #1 and #2, the threat is unlikely to be eliminated, because most potential terrorists expect to terminate themselves. Their goals are to create a loss of confidence in the US government and to force US isolation and withdrawal. Their targets are symbols, economic, infrastructure, and mass casualties. Furthermore, although there is generally broad leeway in Afghanistan and Iraq for IED counter-measures, in the US there are severe legal and social constraints.

For Finding #3, it was noted that the report was an assessment, so it is very critical of DHS and other federal organizations. The observation for Finding #4 was that most of the effort is in getting the device, so there is a need to continue to push interest and investment further to the left of the actual detonation. Finding #5 noted that S&T needs to better prepare first responders for the long term. Most of the first responders are volunteers so it is difficult for them to devote a lot of time to their jobs as first responders. This is very different from being a full-time federal employee, whose sole job it is to act as a first responder.

Finally, for Finding #6, S&T currently has inadequate R&D programs to support rapid restoration of social and economic activities after an IED attack.

Next, the leaders of the three HSSTAC Panels presented their progress.

Program Assessment Panel

Dr. Lawrence Papay of the Program Assessment panel presented his panel's objective and tasking to review, assess, and make recommendations with regard to relevance and completeness to the Under Secretary for S&T. Seven specific taskings were developed for the panel: 1) review the scope of S&T's mission; 2) evaluate strategic planning and operations; 3) get an understanding the S&T program; 4) review financial performance; 5) assess relationships with other S&T organizations; 6) review S&T directorates and how their process is tracked; and 7) provide recommendations on the health and quality of the S&T programs. Since there are several audiences for this panel's pending report, it can serve as a transition between administrations. Congress also requires updates on an annual basis.

In order to complete its taskings, panel members have talked to S&T Division Directors, the Chief Financial Officer, the Homeland Security Institute, and representatives from first responder organizations; they also plan to talk to Congressional staffers. A timeline was made in March 2008, and they have had meetings in April and June. They have been in fact-finding mode until now, and will start talking about where to go next and begin drafting the report in August.

Cyber Threat Response Panel

Dr. Richard Roca is the chair of the Cyber Threat Response panel. The panel's concern is the fact that the cyber domain is dynamic and evolving, so a constant evolution in the

measures taken to protect and defend it is necessary. The question becomes how technology informs procurement for various mechanisms. Multi-level security is involved, and the focus is on the reconstitution, remediation, and response to potential threats.

Cyber protection was compared to the anti-submarine program in the Navy, and the question was asked: Is there an analogous application (physics-driven) that can be used in the cyber world? There are several complications to government adapting to technological changes. Moore's law states that the government takes 18-24 months to adjust and adopt a new technology. However, by that point, the technology is already obsolete and more technologically advanced adversaries have already adjusted and adapted to a faster and more dangerous form of technology. The final panel report on cyber security will outline the issues and discuss what long-term investigations should focus on.

ChemBio Panel

The third panel, the ChemBio panel, is chaired by Dr. David Franz. Dr. Franz presented the timeline for the ChemBio Report, giving August 1st as the deadline to have the draft completed. Before 1997, all ChemBio defense work was done in DoD. There was a $37 million budget until 9/11; afterwards, this number jumped into the billions. The terms of reference for this committee were to understand the form and function of S&T but focus on the seams between assets and stakeholders within and outside of DHS. Dr. Franz then presented the mission, 5-year deliverables, and recommendations that the report will include.

The panel briefings concluded this meeting. The next meeting of the HSSTAC will be on October 20-22, 2008 in Norfolk, VA.

Ervin Kapos
Designated Federal Officer