STATEMENT FOR THE RECORD

FOR

THE JOINT 9/11 INQUIRY

17 October 2002

DIA RESPONSE TO JOINT 9/11 LETTER OF INVITATION

Rear Admiral Lowell E. Jacoby, US Navy
Acting Director, Defense Intelligence Agency

Statement for Record

Rear Admiral Lowell E. Jacoby, United States Navy

Acting Director, Defense Intelligence Agency

10 October 2002

Chairman Graham, Chairman Goss, members of these Committees, thank you for another opportunity to address the performance of the Intelligence Community concerning the September 11, 2001 terrorist attacks against the United States. I appreciate your Committees' focus on identifying actions that will strengthen the Intelligence Community, enabling us to better detect and prevent future terrorist attacks.

Rather than repeat the detailed responses from our earlier statements, I want to focus on five lessons-learned concerning the terrorism threat to the United States. In exploring these lessons, I will cover the three general questions posed in your letter – what we could have done differently, what we derived from the experience, and what we are doing about it – as well as the range of specific subjects you requested I address.

> The first and earliest lesson-learned is that we must largely reject previously held assumptions about the magnitude and nature of the terrorist threat to the United States. Similarly, we must constantly and methodically reassess current assumptions about terrorists' operational behavior and decision-making.
>
> Next, as a community, we must work as a unified body to focus on the threat and not allow organizational, jurisdictional, or territorial boundaries to diminish the effectiveness of our efforts. We must close any intra-governmental seams that can be exploited by an adaptive, transnational, and elusive adversary.
>
> Third, we must reengineer the community's information management paradigm. Information is the raw material of the intelligence business and we must find ways to extract additional value from what is currently available while at the same time harvesting and exploiting new and non-traditional sources of data.

Fourth, we can take little comfort in strategic warning where the threat of terrorism is concerned. The nature of the threat demands warning with tactical perspective, timeliness, and specificity. A natural tendency to "over-warn" must be recognized and overcome.

And finally, the war on terrorism is a long-term proposition that demands extraordinary continuity of purpose, focus, and resource commitment. We cannot allow a lull in terrorist attacks – no matter how long it might extend – to engender a false sense of security and a lowering of priority.

Prior to the 11 September attacks, terrorist operations against United States' interests were not seen as posing a grave threat to the national security of the United States. I am not downplaying the gravity of these attacks, as they had serious and tragic impact on our activities, people, and interests overseas. However, the 11 September strikes at the core of America's military, political, and economic systems changed forever the way we view the terrorist threat.

We were surprised analytically by the complexity of the overall plan, the stunning simplicity of "weaponizing" for mass casualties, and the benign backgrounds of the individual attackers. Our underlying assumptions about bin Ladin's creativity and limits on his actions were wrong. In short, long-held analytic assumptions about terrorist groups and their intentions, values, constraints, and methods of operation – which were challenged by the earlier attack on the USS COLE -- were completely shattered on 11 September.

Maintaining a government-wide, carefully orchestrated counterterrorism effort is critical. Terrorists not only recognize and respect no geographic boundaries; they are committed to aggressively discerning cracks, or seams, in our defenses. Jurisdictional -- and sometimes "turf" -- lines between foreign intelligence activities and law enforcement responsibilities, particularly in the domestic context, represents that type of potential seam.

While the hand-off mechanisms between and among intelligence and law enforcement agencies work fairly well, they have to extend further and become more institutionalized. In doing that, we must ensure a steady flow of information, expertise, and insight both horizontally and vertically – that is, from National to State to Local, and the reverse. I recognize and accept that some information cannot be fully shared. But, what can be shared must be shared.

Our measures of success must lie in the area of effectiveness, not efficiency. While some issues are prime candidates for cross-community economizing – i.e. distributed or federated analysis, product deconfliction, strict division of labor– terrorism is not one of them. Some of the potential seams in our defenses may best be closed by overlapping efforts and responsibilities. Terrorism is an issue where competitive analysis is essential; planned duplication and redundancy by design are virtues.

The benefit of competitive analysis is optimized only when all parties have access to the same information base. The act of drawing different – even opposing – conclusions from a common body of evidence should be encouraged. It is an opportunity to extract additional "meaning" from fragmentary data, ultimately increasing the precision and impact of our collective threat analyses. I remain steadfast in my belief – elaborated upon in previous statements -- that the analytic component of the Intelligence Community can make a greater contribution to the war on terrorism if given access to a much wider range of information and supported with more capable technologic tools.

One part of gaining wider access to potentially relevant information is technology-based; the others are cultural or procedural. On the technology front, we are moving our Joint Intelligence Task Force for Combating Terrorism (JITF-CT) into a completely transformed information management environment based on best practices and standards of the commercial sector. By transitioning to eXtensible Markup

Language (XML) standards and initiating data-tagging at the content level, we can begin reaping the substantial benefits of modern data mining and "analytic discovery" tools. Our ultimate objective is to achieve interoperability at the data level, rather than the system level.

In short, we know we can improve the power and performance of existing information and, at the same time, prepare to assimilate and exploit new sources and types of information to which we are seeking greater access. Since 11 September, the JITF-CT has achieved much greater access to some types of information and progress is being made on others. We are committed to incorporating a wider range of previously under-tapped law enforcement/security information into JITF-CT's analyses and see no insurmountable obstacles to doing so. Of note, doing so requires re-defining the traditional view of intelligence collection when it comes to terrorism.

In discerning terrorist intentions and to provide tactical warning, it is desperately important that we harvest and exploit more information on terrorists' pre-incident behavior and activity. There are scores – in some cases hundreds – of discrete steps taken by terrorists as they choose, plan, and move in on a target. For the most part, each step, when observed in isolation, may appear to be everyday, routine activity. For example, the purchase or forgery of travel documents, "accidental" intrusions in secure areas, or movement of cash may have innocent explanations and benign implications. But maybe not.

During the pre-incident period, potential indications of terrorist activities are far more likely to be observed by police, security, or bystanders than by traditional intelligence collectors. We need to do a much better job of incorporating this type of information into our analytic equation. While ninety-nine percent of it will likely turn out to be "noise," we cannot afford to miss the one percent that is not. Provision of tactical warning is dependent on receiving and understanding tactical-level indicators.

Once analysis of indicators reveals a threat, the next step is, of course, timely dissemination of warning. Much like the collection arena, the indications and warning arena for terrorism poses unique dilemmas for the community. For many issues, we judge the effectiveness of our warning efforts by the accuracy rate of our predictions – i.e. of the events forecasted, how many did, in fact, occur? In predictions, an eighty percent accuracy rate is considered very commendable. Conversely, terrorism warning, when effective, causes action to be taken which prevents the event. A predictive accuracy rate of zero is the desired goal. Prevention, not prediction, is the measure of effectiveness for terrorism warning.

The Defense Intelligence Agency has invested heavily in terrorism warning. Force Protection has been, and will continue to be, among our most important missions. In that regard, the "*Report of the DOD Commission on the Beirut International Airport (BIA) Terrorist Act, 23 October 1983,*" (Long Commission Report), continues to serve as the prevailing benchmark for our terrorism warning efforts. Among the intelligence inadequacies documented in that report was the injudicious issuance of a constant stream of "chicken little" warnings.

Over-warning – particularly the broad dissemination of generalized, non-actionable alerts – unquestionably degrades and ultimately subverts the intent and effect of the warning process. On that note, I should point out that the Intelligence Community's guidelines for issuing terrorist threat alerts and advisories are exactly right. Collectively, we must exercise the discipline to adhere to them.

Discipline may also be required to ensure we sustain the momentum, focus, and resources needed for an extended, war on terrorism. Unfortunately, governmental attention on terrorism has been episodic, rising sharply in the aftermath of major events – such as the downing of Pan Am Flight 103 or the attacks on our embassies, Khobar Towers, and USS COLE – and declining noticeably as the months pass without an additional attack. In some cases, resources that were apportioned to address the threat of terrorism were diverted or diluted as soon as the episodes of high attention subsided.

Since 11 September, the U.S. has employed extraordinary security measures at home and abroad. We have enjoyed unprecedented cooperation on terrorism intelligence and security issues from governments across the globe. Within our own government, we devised new ways to cooperate and collaborate and have allotted very significant resources and energy to the war on terrorism. Great progress has been made. The result of our collective effort is a particularly difficult operating environment for terrorists.

However, as history shows, terrorists work on their own timelines. They are content to wait months or years to increase their chances of success or the lethality of a specific action. In many ways, terrorism is like a cancer that invades an unsuspecting body even as it appears free of outward symptoms. A prolonged lull in terrorist attacks does not infer a diminished threat. In fact, akin to the paradox inherent in terrorism warning – a preventive not predictive process that seeks zero percent predictive accuracy – it is not difficult to argue that the longer we go with out a major attack, the closer we are to the next one. Constancy of purpose, continuity of focus, and unity of effort must be our watchwords. Thank you.