STATEMENT FOR THE RECORD

FOR

THE JOINT 9/11 INQUIRY

1 October 2002

INFORMATION SHARING OF TERRORISM-RELATED DATA

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

Statement for the Record
Rear Admiral Lowell E. Jacoby, United States Navy
Acting Director, Defense Intelligence Agency
1 October 2002

Chairman Graham, Chairman Goss, and Members of these Committees: thank you for the opportunity to address the issue of sharing terrorism-related information. It is a topic of exceptional importance and one upon which DIA has focused considerable attention in an effort to enhance our analytic approach and capabilities for the War on Terrorism. As requested, this statement is structured around the specific questions contained in your September 17, 2002 letter.

Very shortly after the terrorist attack on the USS COLE in October 2000, DIA took steps to significantly alter its structures, processes, products, and conventions associated with analysis of terrorism. We recognized at that time that the terrorist threat had evolved and changed in very complex ways and that our analytic approach had not kept pace with those changes. The steps we took were based on two fundamental beliefs: that analysis, conducted in true all-source mode, could make greater contributions to the counterterrorism mission; and, that significant amounts of information with relevance to the terrorist threat were under-utilized, essentially not subjected to analytic scrutiny and exploitation.

We understood that we were not optimally configured – in terms of policies, procedures, and technology -- to accommodate the receipt and rapid exploitation of that under-tapped information. Consequently, we fielded the mechanisms needed to obviate several factors that had limited our ability to receive some categories of information. These factors ranged from strict compartmentation and law enforcement concerns to sheer volume and fragmentation of data. With the standup of the Joint Intelligence Task Force for Combating Terrorism (JITF-CT) and its associated "limited access data

repositories," leading-edge information handling technology, and consolidated analytic cadre, we are close to being optimally configured to receive information from any and all sources.

The JITF-CT is a consolidated national-level Department of Defense (DOD) all-source intelligence fusion center staffed, equipped, and directed to support an aggressive, long-term, worldwide campaign against terrorism. The JITF-CT is designed to support the full range of DOD efforts to combat terrorism, both offensive and defensive, with particular focus on providing strategic and tactical warning, exposing and exploiting terrorist vulnerabilities, and preventing terrorists and their sponsors from acquiring increased capabilities, particularly in the area of weapons of mass destruction.

The single most critical goal of the JITF-CT is fielding of a stand-alone, limited access data repository accredited to host the entire range of terrorism related information, regardless of source. No such repository of information exists within the Department of Defense today. Categories of information often not subjected to all-source intelligence analysis today include some highly compartmented intelligence, law enforcement information related to ongoing investigations or prosecutions, and security incident reporting sometimes catalogued as criminal, rather than terrorism activity.

The JITF-CT intends to not only capture this information but to apply state-of-the-practice technological tools and expertise that enhance opportunities for "analytic discovery." For example, commercially available tools can help discern and understand obscure linkages between individuals, activities, and methods in the pre-attack phase of a terrorist operation, even if it stretches over years and several continents. Using commercial technology, the JITF-CT will sustain a terrorism analysis effort that dramatically modernizes the way it accesses, stores, manipulates, interprets, and disseminates information.

Successes in deterring terrorist attacks will most always involve some combination of intelligence, good police or investigative work, vigilant security, foreign government involvement, and plain luck. With the exception of luck, each of these entities possesses knowledge and information not ordinarily available to the intelligence analyst. Trends in terrorist organizational and operational behavior – loosely affiliated groups and collaborative planning or execution of operations, often geographically dispersed and stretching over long periods of time – combined with their small footprint and extraordinary efforts to conceal their activities argue that terrorism-related information will nearly always appear to be fragmentary, ambiguous, and uncorroborated.

In our search for relevant information, we must cast a much wider net and then more rigorously mine, manipulate, and interpret the take. In terms of the now-popular analogy of "connecting the dots," we must assume that some of those "dots" are to be found in the observations of gate guards, investigations of thefts and break-ins, or the seemingly benign conversations between terrorist supporters and sympathizers. We simply cannot allow a "dot" to be overlooked, regardless of where it might be found or how deeply imbedded in noise or obscured by faulty assumptions about its nature and relevance.

At its most basic, intelligence analysis is a relatively binary process wherein evidence – observed, reported facts/activities – is combined with assumptions – analytic insight, knowledge – to create an assessment. In essence, the terrorism analyst's job is the extraction of "meaning" from incomplete evidence, using knowledge, experience, expertise and insight to compensate for absent evidence and ever-present ambiguity.

As more powerful and diverse assumptions are applied to the evidentiary base, more powerful and precise assessments are produced. The only certain way to increase the breadth and diversity of assumptions is to increase the breadth and diversity (in terms of educational and experiential background,

cultural values, intellectual biases, etc.) of the analysts involved in the assessment process. In this regard, the more widely fragmentary information is shared, the more likely its hidden meaning will be revealed. Information considered irrelevant noise by one set of analysts may provide critical clues or reveal significant relationships when subjected to analytic scrutiny by another. This process is critical for the terrorism issue where evidence is particularly scant, often separated by space and time.

As an active and vocal advocate of collaborative analysis and increased sharing of information, DIA knows the importance of close community cooperation and is an active participant in the terrorism intelligence community. We have backed up our commitment to analytic partnership by assigning experienced terrorism analysts to other counterterrorism organizations. We currently have analysts deployed in support of interrogation efforts in Afghanistan and at Guantanamo Bay. The JITF-CT has experienced terrorism analysts assigned to counterterrorism components of CIA, FBI and NSA. As new personnel are hired and trained, we will begin deploying JITF-CT terrorism analysts to the Combatant Command Joint Intelligence Centers.

Of note, the JITF-CT charter lists "Bridging Interagency Terrorism Intelligence Efforts" as one of its primary functions. Through assignment of JITF-CT personnel to, and hosting personnel from, other US government elements engaged in the campaign against terrorism, the JITF-CT seeks to ensure DOD is aware of and able to assist, benefit from, and coordinate relevant antiterrorism and counterterrorism intelligence efforts throughout the US government. In this regard, DIA maintains longstanding and active participation in the Interagency Intelligence Committee on Terrorism.

Historically, we've had mixed results regarding the effectiveness of community partnerships. The mere act of assigning an analyst to another organization does not ensure a greater level of access to information or more

open sharing of information. JITF-CT analysts in counterpart organizations do not have unfettered and unconditional access to all relevant terrorist information. By virtue of their status, these analysts are unquestionably afforded greater access to host-agency data; but, in some cases, they are restricted from making that additional information available to colleagues at their home agency. As such, some of the tangible benefits and explicit objectives of exchanging personnel – sharing of information and leveraging collective expertise – are degraded. However, real progress has been made in the past year and I am optimistic that the full benefits and objectives of community integration will ultimately be realized.

In response to your specific question about information sharing, DIA does not have access to all intelligence and law enforcement information on terrorists. I cannot quantitatively or qualitatively assess the percentage of "missing" information; I can't know what I don't know. Nor can I precisely describe the limits or the basis for those limitations regarding information that is withheld from DIA. I respectfully suggest that explanations should more appropriately come from those intelligence and law enforcement organizations that are the "owners" or "arbiters" of unshared information. That being said, I want to emphasize that I do not believe any information "owner" has failed to rapidly share even a shred of information that it deems as conveying either an explicit or implicit threat to United States citizens or activities. I believe the un-shared information falls largely into the categories of background or contextual data, sourcing, seemingly benign activities, and the like. But, as previously mentioned, it is within these categories that the critical "connecting dot" may well be found.

Also in response to one of your specific questions, I am not aware of any legal or policy obstacle to DIA sharing information related to terrorism, suspected terrorists, and their associates. We are, of course, subject to a range of intelligence oversight policies and procedures that impose some restrictions, most notably those pertaining to United States citizens, but we are not

constrained from performing our foreign intelligence or force protection missions. Laws and governing directives provide sufficient flexibility and, properly interpreted and complied with, do not inhibit our ability to share or receive information relevant to the terrorist threat.

DIA has a longstanding commitment to share and widely disseminate the results of its terrorism analysis. The JITF-CT currently maintains an extensive terrorism database that dates back to the mid-1980s and fulfills intelligence production responsibilities established in DOD directives. This database was established principally to provide our customers with baseline terrorist threat and modus operandi analysis in support of the force protection (antiterrorism, prevention) mission. It is neither designed nor used for tracking suspected terrorist movements in the United States or abroad. The finished intelligence contained in our data base – for example, over 10,000 biographic profiles, 190 terrorist group profiles, over 8,000 incident summaries, and current threat assessments for every country in the world – is available on-line to anyone with access to DOD intelligence networks. As you can imagine, this represents a serious resource investment that underscores our deep commitment to information sharing.

During my interview with the Joint Inquiry Staff, I stated that one significant change needed was to create a new paradigm wherein "ownership" of information belonged with the analysts and not the collectors. In my opinion, one of the most prolonged and troubling trends in the Intelligence Community is the degree to which analysts -- while being expected to incorporate the full range of source information into their assessments -- have been systematically separated from the raw material of their trade. In fact, while I acknowledge there are many pockets where groundbreaking, innovative, true all-source analysis is occurring, they are the exception, not the rule. I don't make this statement lightly and it is not my intent to offend or disparage the quality of our analysts or the competence of their management, because -- of course -- I'm part of that latter group.

There are good and very understandable reasons why our all-source analysis effort is in this situation. Large analytic workforce drawdowns of the early 90's combined with voluminous streams of collected data required more "front end" filtering of raw information, thus moving the interpretive functions of analysis– the extraction of meaning from data – further inside the collecting organizations. This is not necessarily a bad thing. And, I have great respect for those in the processing and exploitation arena who labor to separate the nuggets from the noise, to rationalize the irrational, and to add meaning. Theirs is an indispensable and value-adding function.

However, when so-called all-source analysts are put in the position of basing important judgments on "some-source" or "already-interpreted-source" information that is a bad thing. I need to be clear in stating that I am referring to access to collected data, not unfettered access to source data, particularly the areas of law enforcement and human sources. On exceptionally difficult issues such as terrorism analysis, where the available information is by its very nature fragmentary and episodic, we need to find a way to immediately and emphatically put the "all" back into all-source analysis.

If we expect analysts to perform at the level and speed expected in a counterterrorism mission environment characterized by pop-up threats, fleeting targets, and heavily veiled communication, they require immediate, on-demand access to data from all sources and the ability to mine, manipulate, integrate, and display all relevant information. What I envision is a different way of doing business in the Intelligence and Law Enforcement communities. Make no mistake; it would involve unfamiliar processes, partnerships, and prerogatives.

While broader access to data is the one of the keys to changing the paradigm, another important step is more effective management and exploitation of information. Before we can field successful information management

strategies, we must first put our information in a form and into an environment where it can, in fact, be managed.

Information Management is an area where we should take our lead from the commercial sector. After all, profits and losses of information-fueled businesses outside of government are determined by how they manage information. Those who are successful in a business sense -- showing real rather than paper profit -- certainly have some lessons to teach us.

If we are to achieve an end state characterized by the ability to rapidly share and integrate information, we must move toward a common data framework and set of standards that will allow interoperability – at the data, not system, level. In my view, the commercial world's collective embrace of eXtensible Markup Language – XML – standards is precisely what we should do. And, the sooner the better, not just for a limited group of intelligence producers and subsets of data; it shouldn't be an elective option. Interoperability at the data level is an absolutely necessary attribute of a transformed intelligence environment because it enables horizontal integration of information from all sources – not just intelligence – and at all levels of classification.

Since 11 September 2001, there have been significant improvements in a number of areas related to information sharing. DIA has made notable arrangements with other Intelligence Community partners to achieve new levels of data access and integration. In other cases, we still have work to do both technologically and procedurally within the JITF-CT and in breaking down external barriers to full sharing.

But, I am exceptionally optimistic. The Director of Central Intelligence expressed his commitment by emphasizing that full sharing of unfiltered, aggregated, and interpreted collected information is a necessary ingredient for victory in the war on terrorism and that anything short of full sharing of such

information ultimately hampers our ability to protect the citizens and interests of the United States. I'm with him.