

13 July 2004

**Statement for the Record of  
Russell E. Travers**

**Deputy Director for Information Sharing and Knowledge  
Development  
Terrorist Threat Integration Center (TTIC)**

**On**

**Facilitating an Enhanced Information Sharing Network that  
Links Law Enforcement and Homeland Security for Federal,  
State and Local Governments**

**Before**

**House Government Reform Committee's Subcommittee on  
Technology, Information Policy, Intergovernmental Relations  
and the Census**

**Washington D.C.**

Good afternoon, Chairman Putnam and Members of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.

I appreciate the opportunity to join my colleagues from the Department of Homeland Security and the Federal Bureau of Investigation to address the initiatives and strategies being implemented to enhance information sharing capabilities between and among Federal, State and local law enforcement agencies and Homeland Security activities. The role of the Terrorist Threat Integration Center in facilitating such sharing is directly related to our mission as laid out initially in the President's 2003 State of the Union Address and as clarified over the past 18 months. Accordingly, I will briefly lay out that mission, as well as TTIC's view of the way ahead. I'll then turn to Information Sharing, focusing on three major aspects: TTIC's access to information, TTIC's role in horizontal information sharing across the federal structures, and TTIC's support to vertical information sharing down to State and Local entities. Finally, I'll close with a few general observations about information sharing and what we should - and shouldn't - expect from it.

## **TTIC and the Way Ahead**

As the Subcommittee knows, TTIC stood up in May of last year, four months after the President's speech. Chartered as a multi-agency joint venture, TTIC is tasked with integrating and analyzing terrorist threat-related information collected domestically and abroad, and then disseminating this information and analysis to appropriate recipients, consistent with applicable privacy and civil liberty requirements. We began operations with approximately fifty U.S. Government staff and have almost tripled in size since then. We have recently relocated from CIA Headquarters to a new facility where we will be joined by large elements of the Director of Central Intelligence's Counterterrorism Center and the FBI's Counter-terrorism Division later this summer and fall. Along with very broad access to information, a great strength of TTIC is the fact that we have had analysts from 16 separate organizations carrying out the work of their parent organization, building bridges between departments and agencies, and enabling us to carry out our mission. These assignees come from a wide array of the key organizations involved in the war against global terrorism, including FBI, CIA, NSA, National Geospatial-Intelligence Agency, Defense Intelligence Agency, the Department of State, Department of Energy and DHS. We also have had a Capitol Police Officer and a representative of the Nuclear Regulatory Commission. This broad representation will continue to grow as TTIC expands. These individuals bring with them unique expertise and connectivity to their home organizations.

Despite the predictable challenges with the standup of such a complex organization, TTIC has enjoyed significant success in its primary analytic and reporting function; in the past 14 months we have produced over 300 Presidential Terrorist Threat Reports for our senior leadership, 400 Terrorist Threat Matrices, 500 Terrorist Situational Summaries as well as scores of unique products dealing with terrorist threat warning and other issues.

In the past, numerous organizations were trying to "do it all" regarding terrorism analysis, and with that came relatively shallow analysis and an inability to delve deeply into issues. TTIC's creation and stand-up has helped alleviate that problem by concentrating the

responsibility for terrorism analysis within the USG. As described in the recent response to a letter from Senators Collins and Levin:

“TTIC has the primary responsibility in the USG for terrorism analysis (except information relating solely to purely domestic terrorism) and is responsible for the day-to-day terrorism analysis provided to the President and other senior policy makers.”

We are now working with the Community to gain the resourcing necessary to successfully carry out that mission. The CIA has already promised to detail 60 additional officers to TTIC as soon as possible. At the same time, Memoranda of Agreement are being staffed with the relevant Departments and Agencies in order that we might be assigned the necessary quantity and quality of experienced terrorism analysts. While additional work is required to fully determine the scope and migration of resources necessary to meet this expansive mission, we have, in partnership with other elements of the USG, made notable progress.

#### **TTIC and Information Sharing**

There is no question that information sharing is at the heart of TTIC's mission. As mandated in DCID 2/4, TTIC is to “create a structure to institutionalize sharing across appropriate federal agency lines of terrorist threat-related information, collected domestically or abroad in order to form the most comprehensive possible threat picture and minimize any seams between analysis of terrorist threat related information and minimize any seams between analysis of terrorist threat related information collected domestically or abroad.” While this will always be a work in progress and much is yet to be accomplished, TTIC and the entire USG have made substantial progress since 9/11 overcoming numerous impediments to information sharing.

To begin with, a solid legal and policy groundwork for information sharing has been put in place since 2001: the USA PATRIOT Act; the Homeland Security Act; the Presidential decision to create the Terrorist Threat Integration Center; the Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security

Concerning Information Sharing; the Director of Central Intelligence Directive establishing TTIC; Homeland Security Presidential Directive 6 creating the Terrorist Screening Center; and the first of a new series of DCI Directives pertaining to Information Sharing, DCID 8/1 Intelligence Community Policy on Intelligence Information Sharing, have all played a role in driving the improvements in sharing terrorism-related information.

With the underlying legal and policy framework in place, the Community has been focusing on the new business practices, cultural changes, and technical systems needed to fully implement these policies. Both in terms of the absolute amounts of available reporting and the extent to which it is widely shared in the Community, the government has made substantial strides. For example, if we compare intelligence reporting on terrorism-related subjects now, with reporting in 2001, we see tremendous growth. Immediately after the terrorist attacks on September 11, 2001, purely terrorism-related intelligence reporting surged, from an average of roughly 300 per day in early 2001, to an average of approximately 850 reports per day in late 2001. Since that time, the amount of intelligence reporting on terrorism related issues has continued to increase to about 1,700 per day in 2004. More importantly, because of the technical, cultural and business practice changes that are starting to take place, that information is being widely disseminated to those intelligence, law enforcement, and homeland security analysts who need to see it.

TTIC takes its responsibilities in the information-sharing arena very seriously. Beyond the core business function of integrated analysis and the associated Department focused on Analysis and Production for the entire Community, TTIC has three organizations that are directly involved in information sharing:

- TTIC's CIO has worked closely with the Community CIOs and all relevant partners to ensure that the proper architecture and standards are in place to support the mission of terrorism analysis. Our CIO's extraordinary work has been amongst the most visible of TTIC's successes, receiving wide acclaim across the community. In particular, TTIC Online, which will be discussed below, has become the principal source of

all source terrorism analysis for the entire community.

- TTIC stood up an Information Sharing Program Office in mid-2003 to oversee implementation of the Information Sharing MOU. Our focus has been on the key impediments to a free flow of terrorism-related information, including such issues as "Originator Controlled Information", "the Third Agency Rule", "No Double Standard" rule and so forth. Such control mechanisms have their place, if properly used, but by definition also impede information sharing. TTIC is working with the Community to reduce these impediments to the absolute minimum: one metric of success - the use of ORCON has declined across the Community by about 40% since 9/11.

- And recently, TTIC and DIA have established a Force Protection Cell, staffed by DoD assignees to TTIC. These individuals will have complete access to all information available to TTIC and will focus on that reporting that might be relevant to DoD's force protection requirements around the globe. Once identifying such reporting, they will work the modalities to ensure rapid dissemination to the Defense Department. TTIC believes this could be a useful model for other Departments and Agencies to follow.

### **TTIC and Access to Information**

As the U.S. Government's Terrorist Threat Integration Center, it is imperative that TTIC have access to all relevant information. This notion was captured in our chartering document, Director of Central Intelligence Directive 2/4, which called for TTIC analysts to have "unfettered access" to terrorism threat-related information. Operating under that guidance, TTIC has been working with information providers from across the government to gain access to all appropriate information.

As depicted below, TTIC assignees with the appropriate need to know currently have access to up to 21 networks from across the intelligence, law enforcement and homeland security communities. With our recent move to the new building this figure will soon grow to 26 separate networks.



# Our Access: TTIC Network Connectivity



\*Not all analysts access all networks or tools; Mission requirements determine access.

\*\*Planned networks: ION, NCIC, NRO GWAN, JCON, OASIS

\*\*\* Dial-Up networks currently available in TTIC: Secret Service, DHS TECS, DHS ICE, USCG Intranet

Over the past year TTIC has worked with the various partner organizations to broaden individual analyst access to these 21 networks. At standup, for example, access to CIA operational traffic was limited largely to CIA analysts and access to FBI's network was limited to FBI analysts. This has changed dramatically, and now, appropriate analysts from across the Community, once they have received necessary training, are able to access other organizations' networks.

The upshot of such broad access is that an analyst may well have six or more CPUs under his or her desk - thereby raising an entirely separate set of problems: simply put, an analyst will have to switch from network to network in order to pursue a line of inquiry against various Agency data bases and intelligence holdings. This is an extremely inefficient and time-consuming process, and runs the risk of incomplete analysis. Nevertheless, historically, this has been necessitated by the differing architectures and

security protocols associated with the relevant Departments and Agencies.

TTIC's CIO recognized this problem very early on and has been working on an architectural solution that will allow a federated search - one query against the holdings on multiple systems. Expected to reach initial operating capability in the next month, our approach, called Sanctum, will allow analysts to search against the holdings of five systems; this will gradually expand over time and will help analysts deal with the information overload problem.

Mr. Chairman, it would be premature to declare victory regarding TTIC's access to information. We are still dealing with a host of challenges, ranging from a disparity in technical capabilities of networks across the government, to various Special Access Programs and other highly restricted categories of material, to basic questions about whether TTIC should have certain types of information, to protocols and procedures that govern the flow of information. And while we continue to work these issues, I am confident in saying that nowhere else in the government brings together such a diverse set of intelligence, law enforcement and homeland security information associated with the terrorism problem.

### **TTIC Initiatives in Information Sharing**

Information sharing has both horizontal and vertical components. TTIC's primary focus is on the horizontal aspects - ensuring that the Federal structures have the required information to fulfill their missions. Vertical information sharing is worked more directly by the FBI and DHS.

To begin to bridge the cultural gaps between the Intelligence, law enforcement and Homeland Security communities in the Federal Government, TTIC organized and sponsored its first Terrorism Information Sharing conference for the Federal Government in late March 2004. This classified conference was designed to attract professional mid-level decision makers from across the Federal Government who work in the fight against terrorism. The conference was a success, drawing over 260 participants from 40 different Federal organizations. We still have a long way to go to bridge the cultural gaps between different communities of counterterrorism professionals,

but this conference was a good first step. It dispelled many misunderstandings, raised the general level of knowledge and mutual understanding among participants, and pointed out the areas where we still have work to do.

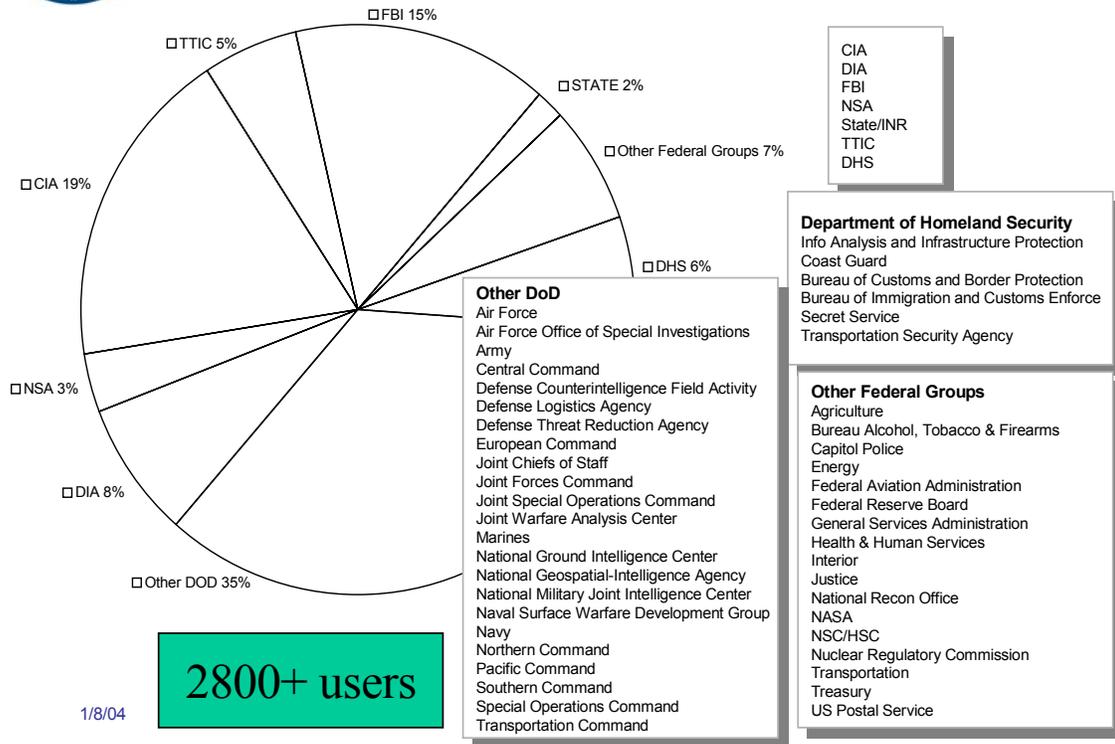
### **TTIC Online in Support of Horizontal Information Sharing**

One key initiative that reflects our progress can be seen in the ability to electronically access terrorist-related information. Over the past 14 months TTIC has focused on the technical initiatives necessary to promote information sharing. Because of our mission, we are in the unique position of having to improve our ability to manage information, while creating an environment in which analysts can benefit from a diverse array of Intelligence Community and law enforcement sources. These demands require an architectural approach that makes best use of extant technology and legacy systems while ensuring smooth insertion of emerging technology in the future.

To promote horizontal information sharing across the entire Community of analysts working the terrorism problem, we launched the TTIC Online (TTOL) website in August 2003 leveraging and building upon CT Link, a secure community of interest created by CIA's Counterterrorist Center. The TTOL website now serves as the front door for the Intelligence, Law Enforcement, Homeland Security and Military communities to access a broad range of counterterrorism threat information. This highly secure capability can reach virtually the entire structure of the Federal Government, hosting over 2800 users in the JWICS Top Secret community. TTOL reaches not only the traditional national Intelligence Community terrorism analytic elements, but also the JTTFs, the military Commands, and numerous entities outside the Intelligence Community that have a need for terrorism-related information. The current breakout of the population of TTOL users and the full range of organizations that access the network can be seen below.



# USG Wide Reach of TTIC ONLINE



TTIC Online contains approximately 3.5 million documents, including finished intelligence from CIA, TTIC, DHS, and FBI; disseminated reports from the Intelligence Community; access to a repository of tearlines from CIA, NSA, and DoD; warnings, alerts, and bulletins issued by FBI, DHS, and others; and links to other terrorist-threat resources on INTELINK. TTIC Online also hosts the USG database on known and suspected terrorists for which TTIC has responsibility; known as TIPOFF Web this provides, for the first time, a single, widely accessible database on known and suspected international terrorists.

The following chart further illustrates the extent to which our changing business practices, further enabled by technology, have substantially improved overall information sharing across the Community.

<b>From CT Link to TTIC Online: 9/2001-6/2004</b>	
<b>September 2001</b>	<b>June 2004</b>
471 Active users	2838 Active users
10 Users per month add rate	100 Users per month add rate
29 Active organizations	120 Active organizations
20 Sessions per week	1000+ Sessions per week
200 Document hits per week	88,000+ Document hits per week
4 Product types	92 Product types
14 FBI/LE reports per month	450 FBI/LE reports per month
1 Million document repository	3.5 Million document repository

In May of this year we launched a new version of TTIC Online at the SECRET level that is available to a much wider group of users across the Federal Government. This new presence on SIPRNet makes Secret level counterterrorism information available to a wide array of DoD, DHS, law enforcement and Department of State users; this new audience is many times the size of the original user base, and as such, the SIPRNet version of TTIC Online will be of tremendous value to us in moving information outside of the Intelligence Community.

### **Vertical Information Sharing**

As noted above, by DCID, TTIC is primarily focused on promoting horizontal information sharing with Federal organizations. Recognizing the importance of vertical information sharing, we are doing everything possible to support the FBI and DHS in their efforts to push information to state, local, and private sector entities. Two initiatives, in particular, bear mentioning:

- Along with the Top Secret and Secret versions of TTIC Online, TTIC also plans to deploy a Sensitive But Unclassified (SBU) presence of TTIC Online on the Open Source Information System (OSIS) network. TTIC continues to solicit new users from across the Federal Government, and to add new sources of counterterrorism information. This should be instrumental in assisting FBI and DHS with their vertical information sharing efforts.

- TTIC has been working closely with the Community to increase the use of "Tear Lines", a means by which sanitized material can be shared much more widely with audiences that don't have high-level clearances. By leading the effort to establish common formats and content standards, we anticipate being able to automate tear line procedures and expedite the passage of material.

TTIC also is interested in vertical information sharing from the standpoint of receiving information that could originate at the local level. With the assistance of DHS and FBI there have been successes and advances in this area, however there is a great deal of work to be done. We look forward to working as appropriate with DHS and FBI to further the creation of an over-arching architecture that addresses the full range of issues associated with vertical information flow.

### **Information Sharing In Context: Some Final Observations**

TTIC is second to none when it comes to espousing the importance of information sharing. And, as noted above, while much work is yet to be done, there is absolutely no question that the USG has made huge strides in this area since 9/11. However, having been immersed in the issue since the standup of TTIC, a few cautionary words are in order:

*--Be wary of the bumper sticker:* There seems to be complete agreement across the government on the need for better "information sharing". Conferences are held, editorials are written and pundits wax eloquently, but in reality, once we get below the low hanging fruit, there are very difficult issues involved. The intelligence, law enforcement and homeland security communities are invariably faced with a complicated mix of technical, security, policy and legal challenges associated with improved sharing of information. There are very few easy fixes.

*--Information must be protected as well as shared:*

Attaining the proper balance is the key. There seems to be an underlying current suggesting that all "terrorism-related" information should go to all people that are somehow involved in the USG

counterterrorism effort. Such an approach would likely put at risk sources of information and operations critical to winning the war on terrorism. There will always be source sensitivity issues, operational considerations, counter-intelligence aspects and a host of other security related problems, as well as important privacy issues that will reasonably limit free flow of information.

--*Information Sharing is not a panacea*: In short, information sharing is necessary but not sufficient. If we don't have the basic business process for terrorism analysis right, and haven't established critical mass of analytic talent, we can pass information all over the government and still not connect the proper dots; indeed we could even face the prospect of simply being wrong faster. Terrorism is an extraordinarily difficult analytic problem and the key is having long-term expertise and state-of-the art technical analytic tools able to sort through reams of information, much of which is inaccurate, contradictory or utterly irrelevant.

--*"Effective information sharing"* is critical: We are seeing an explosion of networks and websites, containing terabytes upon terabytes of information. Data tagging may be a small part of the solution (though it has far more applicability to the data end of the spectrum rather than the knowledge end). As Agencies "post" their information, they can legitimately say they have shared the information. Whether anyone on the other end knows how to find it and read it is an entirely different matter.

## **Conclusion**

In conclusion, Mr. Chairman, any objective observer of the situation across the USG would conclude that substantial progress has been made over the past three years. Whether it takes the form of multiple daily secret daily videoconferences among the entire Federal counterterrorism community, the creation of organizations specifically devoted to addressing information sharing impediments, the technological advances allowing increased access to the USG's most sensitive information, or the improvements in policies and procedures to facilitate the flow of information, far more terrorism information is

being shared than ever before. Nevertheless, we have much work to do and have many basic questions to resolve: for example, what is "need to know" in an era of globalization? We believe TTIC provides a forcing function to address many of these complex questions and look forward to working with this subcommittee as we confront these difficult issues.

Thank you and I look forward to any questions you may have.