Confronting the Terrorist Threat to the Homeland: Six Years after 9/11

to the Senate Committee on Homeland Security and Governmental Affairs

10 September 2007

Honorable John Scott Redd

Vice Admiral, U. S. Navy (Ret.)

Director

National Counterterrorism Center

Statement for the Record
by
The Honorable John Scott Redd
Director, National Counterterrorism Center (NCTC)
to the United States Senate Committee on Homeland Security and Governmental Affairs
September 10, 2007

Chairman Lieberman, Ranking Member Collins, distinguished members of the Committee, thank you for the opportunity to testify before you today on our nation's efforts to confront the terrorist threat to the homeland since 9/11.

Since 9/11, sweeping legislative and organizational changes—many of which are attributable to this committee—have fundamentally altered how we protect and defend U.S. interests at home and abroad against terrorism. In particular, the U.S. Government has made substantial progress in building our counterterrorism (CT) capability, developing a strategy based on a detailed understanding of al-Qa'ida and the global movement of violent extremists, and reorganizing the government to remedy the shortfalls revealed by the 9/11 attacks. I will discuss some of these developments with you today.

None of what I will say should be understood to mean that we do not continue to face real and significant challenges. We must continue to improve our intelligence collection on the hardest targets. We must continue to mature our coordination with state and local officials so that the federal government supports their efforts and benefits from their many capabilities. We must better coordinate departmental efforts to counter radicalization both at home and abroad. And we must ensure that departmental planning and budgeting is done in a manner consistent with a U.S. Government-wide effort to counter the terrorist threat we face now and are likely to face in the future.

I would like to briefly review the role NCTC is playing, and will play, to further sustain this progress through enhancing the U.S. Government's capability to detect, disrupt, and deter the threat of terrorism against U.S. interests both at home and abroad.

Today, as directed by the Intelligence Reform and Terrorism Prevention Act (IRTPA), NCTC performs two significant functions in the War on Terror. The first, Intelligence, is a familiar one and one in which I report to the DNI. The second is Strategic Operational Planning. As you are well aware, in this second role I report to the President and am responsible for producing the U.S. Government's overall War Plan for the War on Terror (WOT).

In both roles, NCTC's work is truly an interagency effort. We are part of the ODNI and benefit from his authorities. Our staff includes some 400 U.S. Government employees, the vast majority of whom are on rotation from one of 16 federal departments and agencies, including CIA, DoD, and FBI. This rotational structure is deliberate and embodies the model of "Joint Duty" that has proven so successful within the Department of Defense. By bringing so many departments and agencies together at NCTC, we are able to capitalize on the diverse talents and perspectives that only a truly joint workforce can provide.

I would now like to highlight just a few of the areas in which we've seen improvement over the last few years. I'll speak first to the changes in intelligence and then to those related to strategic operational planning.

In the intelligence area, we have made significant progress translating into action the lessons learned from 9/11 and WMD Commissions. An effective intelligence enterprise requires analysis, information sharing, and interagency collaboration, and NCTC continues to lead the counterterrorism community in all three areas.

Analysis. Analysis is at the heart of the counterterrorism intelligence process, and therefore also at the center of NCTC's mission. Our officers involved in the analytical process understand that their insights and judgments may figure directly in the defense of our nation and our allies. Analysis literally *counters terrorism*: it surveys the battlefield, identifies enemy forces and their intentions, and lays the groundwork for an effective offense and defense that use every instrument of national power—from military force to public diplomacy, and everything in between.

NCTC's analytic mission, as defined by IRTPA, is a broad one. As the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism, with the exception of purely domestic terrorism, our mandate crosses the foreign and domestic divide, and requires us to support the full spectrum of intelligence customers. Central to performing this critical responsibility is providing all of our analysts with intelligence from throughout the U.S. Government. This is, as you know well, a revolutionary concept within the Intelligence Community. But today that concept is reality at NCTC; analysts can and do see sensitive intelligence from the CIA, FBI, Department of Defense, Department of Homeland Security, and other organizations.

This base of knowledge enables us to provide our customers with all-source, integrated analysis. NCTC, in collaboration with a wide array of government partners, generates a spectrum of integrated, analytic products – tailored to the needs and interests of our customers, including the President, Departments and Agencies, and the Congress. Our products range from immediate reports providing situational awareness about largely unevaluated intelligence—for example a daily Threat Matrix and twice daily Situation Reports—to in-depth finished intelligence such as the National Terrorism Bulletin and the President's Daily Brief. Significantly, virtually all of these reports for senior policy makers are coordinated by NCTC, as the DNI's Mission Manager. The purpose of that is to ensure that differing views are not only represented, but that they are also put in context.

NCTC's analytic efforts are not just focused on today's most pressing issue. While we spend significant time analyzing current threat streams to ensure that policy makers are kept fully informed, we also analyze longer-term trends in homegrown terrorism, radicalization, terrorists' use of the Internet, and future terrorists' tactics and weapons. In short, we seek to inform on the full range of terrorism topics.

One of the ways in which we ensure policymakers are informed by the best intelligence possible is to provide Intelligence Community-wide coordinated analysis that includes different agencies' views when such differences exist. The Interagency Intelligence Committee on Terrorism (IICT) serves as our primary forum to do this. Although the IICT

existed before 9/11, it has expanded and improved its activities since that time. The chairmanship has also been elevated so it rests with the Director of NCTC. We take very seriously our responsibility to ensure that IICT products fully and faithfully represent dissenting views—should they exist—among agencies.

Finally, NCTC—in conjunction with the DNI—has over the past year sought to best leverage the Intelligence Community's finite analytic resources for counterterrorism. One important corollary to this is to avoid having every agency cover the same issues. To that end, we have identified agency-specific missions, designated lead responsibility for subject areas, and ensured appropriate competitive analysis so that the Intelligence Community is not single-threaded on important issues. This alignment, called the *Analytic Framework for Counterterrorism,* is a tangible recognition that not every agency can cover every topic all the time—and that to try to do so would not serve the U.S. Government well.

The Analytic Framework is focused on four counterterrorism mission areas:

- **Tactical Offense**: Analysis supporting direct action against the terrorist enemy – led by department and agency analytic elements.
- **Tactical Defense**: Analytic warnings of planned terrorist attacks and operations – led by NCTC, and Defense Intelligence Agency (DIA) in the case of threats to U.S. military targets.
- **Strategic Offense**: Analysis to guide national policy and policymakers in countering violent extremism and radical ideology as a threat to our way of life – led by NCTC.
- **Strategic Defense**: Analysis supportive of efforts to reduce our vulnerability to terrorist attacks and future terrorist capabilities – led by NCTC for strategic warnings, and relevant departments and agencies for vulnerability assessments.

One immediate impact of the Framework's adoption has been the shift of some CIA resources to NCTC so that the former can focus on operational support and the latter can concentrate on strategic analysis, such as the "War of Ideas."

Information Sharing. Let me now turn to the second critical piece of our intelligence enterprise—information sharing. NCTC is committed to sharing information quickly, effectively, and consistently.

Under the IRTPA, NCTC has the responsibility "to ensure that agencies, as appropriate, have access to and receive all-source intelligence products needed to execute their counterterrorism plans or perform independent, alternative analysis," and "to ensure that such agencies receive intelligence needed to accomplish their assigned activities." Today I'll highlight four of our principal efforts: sharing intelligence within the federal government, sharing intelligence with state, local, and tribal governments; bringing together departments and agencies to discuss current threats; and, comprehensive watchlisting of individuals of concern.

At the core of our mission is ensuring that all our federal partners have the intelligence they need. Prior to 9/11 there was no comprehensive place to go if an analyst or operator wanted to find all disseminated terrorism intelligence available to the U.S. Government. Today, NCTC Online (NOL) allows more than 60 U.S. Government elements to share information electronically. It serves as a key classified repository and collaboration tool, reaching intelligence, law enforcement, defense, homeland security, foreign affairs and other federal organizations with a counterterrorism mission. It now hosts more than 8,000 authorized users and holds over seven million terrorism documents.

NOL is also available at different levels of classification. This means that even if users are not permitted to see everything, they can automatically see those materials that fit their security clearances. And this capability is particularly important in helping us with the next information sharing initiative—sharing with state, local, and tribal officials.

NCTC's information sharing responsibilities go beyond that of the Federal Government. IRTPA states that the Director of NCTC is responsible for "supporting the Department of Justice and the Department of Homeland Security, and other appropriate agencies, in fulfillment of their responsibilities to disseminate terrorism information to State and local governments." More recently, with the recent passage of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, NCTC has been given additional responsibilities to tailor CT-related information and products for timely passage to state, local, and tribal governments.

As initially proposed as part of the President's ISE Guideline implementation and later directed by the legislation, we are working with FBI, DHS, the Program Manager for the Information Sharing Environment and state and local officials to establish, within NCTC, the Interagency Threat Assessment and Coordination Group (ITACG). Led by a DHS detailee, with a deputy from FBI, this group will provide additional counsel and subject matter expertise to the federal Intelligence Community and facilitate the sharing of intelligence products tailored to the needs of state, local and tribal entities. It will further strengthen the overall national counterterrorism and homeland security effort.

Our information sharing responsibilities also require us to facilitate robust interagency communication about ongoing operations and events. NCTC chairs regular video teleconferences to maintain U.S. Government-wide situational awareness. Intelligence, law enforcement, homeland security, military, and diplomatic officials from roughly 17 U.S. Government organizations come together three times a day, seven days a week, 365 days a year, to exchange information and collaborate on response options. This is a fundamental change: Before 9/11, there was no routine mechanism to maintain situational awareness across the U.S. Government.

Finally, NCTC also plays a pivotal role in the terrorist watchlisting process. For the past four-plus years, NCTC has served as the U.S. Government's central repository for information on international terrorist identities, known as the "Terrorist Identities Datamart Environment," or TIDE for short. The TIDE database includes, to the extent permitted by law, all information the U.S. Government possesses on the identities of individuals known

or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to international terrorism.

The establishment of TIDE marked a major milestone in the nation's CT effort, compiling into one database information on all known and suspected international terrorists. Before 9/11, watchlisting efforts were spread across multiple databases managed by multiple agencies, a significant vulnerability in the nation's efforts to defend against terrorist attack.

Each day, TIDE sends the FBI's Terrorist Screening Center (TSC) a sensitive but unclassified subset of terrorist identifiers to populate the U.S. Government's consolidated watchlist. This consolidated watchlist, in turn, supports efforts to screen, detect, and interdict the travel of known and suspected terrorists here and overseas. These screening efforts encompass the work of consular officers at embassies, Customs and Border Protection (CBP) personnel, law enforcement organizations across the United States, and foreign and domestic air carriers that fly to the United States. So today, an applicant for a State Department visa is checked against the watchlist at a consulate overseas. At U.S. ports of entry, a border crosser's passport, visa, or driver's license is also checked against the CBP's subset of the consolidated watchlist. And at a routine traffic encounter inside the United States, a suspect's identity is checked against the Terrorist Screening Database (TSDB) through the National Crime Information Center. Finally, airline screening personnel review passenger lists for all flights traveling to the United States to identify individuals who are believed to be a threat to civil aviation or the homeland or who should have additional screening prior to boarding a plane.

Examples of the types of activity that warrant an individual's entry into TIDE and terrorist screening systems include:

- Commission of an international terrorist activity;
- Preparation for or planning of international terrorist activity;
- Collection of information on potential targets for international terrorist activity;
- Collection or solicitation of funds or other items of value on behalf of international terrorist organizations or activity;

- Recruitment of members into international terrorist organizations;
- Provision of material support (e.g., safe houses, transportation, communications, funds, false documentation, weapons, or training) to international terrorist organizations; and,
- Membership in or representation of an international terrorist organization.

While the number of names contained in TIDE has grown since its inception in 2003 from approximately 100,000 to over 500,000, this figure represents every identity associated with individuals entered in the database. This distinction is significant because of the multiple aliases and name variants of terrorism suspects. As a result, the number of actual individuals recorded in TIDE is closer to 400,000. And although TIDE continues to grow, individuals' names are also regularly removed when it is determined that they no longer meet the criteria for inclusion. As a result, more than 10,000 names were removed from TIDE in 2006.

Interagency Collaboration. You will note that NCTC's analytic and information sharing efforts are but a part of the larger CT intelligence effort. Let me now turn, then, to the third piece of NCTC's support for CT intelligence—its coordination of the larger counterterrorism intelligence community. As the DNI's "Mission Manager" for counterterrorism, I am responsible for ensuring that all parts of Intelligence Community work toward a coherent, cohesive counterterrorism vision. Let me give you some of examples of IC-wide efforts that NCTC is leading.

First, NCTC orchestrates the counterterrorism National Collection Plan, which identifies information needs and requirements, assesses collector capabilities, and feeds CT requirements into the collection mechanisms. Second, NCTC has conducted the first-ever comprehensive CT analytic workforce analysis. In March of this year, we published *The Counterterrorism Analytic Posture of the Intelligence Community: A Baseline Report*, which gives us a foundation for evaluating the Community of today and developing recommendations for how to position the Community of tomorrow. The results are now being used to implement improved training and retention plans for the Intelligence

Community. We have also developed a systematic "lessons learned" process to capture best practices to improve the efficacy and efficiency of our efforts. We believe that by creating mechanisms to conduct lessons learned studies the CT Community has, over the past year, taken significant steps towards fostering a culture of learning

Thus far I have addressed NCTC's intelligence responsibilities; I would like to turn now to our second role—Strategic Operational Planning (SOP) for the War on Terror.

SOP involves a wide spectrum of planning functions. It bridges the gap between coordinated interagency policy and strategy and tactical operations by departments and agencies to implement that strategy. Essentially, SOP takes interagency planning to a new and much more granular level than we have historically undertaken as a government.

In this role we lead an interagency planning effort that brings all elements of national power to bear in the War on Terror. That includes the full weight of our diplomatic, financial, military, intelligence, homeland security and law enforcement activities. The strategic operational planning effort is new to the U.S. Government. It involves a three-part continuous process: planning, implementation and assessment. NCTC is leading an interagency effort to build processes for all three phases. We've completed the first phase of planning by the CT community, and we're now in the process of guiding the implementation of the plan and assessing its effectiveness.

NCTC's planning efforts span a spectrum from strategic, deliberate planning to more dynamic planning.

The National Implementation Plan (NIP), which was approved by the President in June 2006, is the keystone document for our strategic—or deliberate—planning. The NIP is truly an unprecedented effort to bring together disparate parts of the U.S. Government that have a role in countering terrorism. Building on the President's unclassified National Strategy for Countering Terrorism (NSCT), it incorporates five years of planning, analysis, operations, and successes in the War on Terror. Each of the strategic objectives is further

divided into specific tasks assigned to a Cabinet-level officer for action and other Cabinet officers for support.

The primary value added of the NIP is that it provides a comprehensive, coordinated plan of action that clearly assigns responsibility, sets priorities, illuminates areas of coordination, and provides a framework for assessing success and, ultimately, assigning resources.

In the spectrum of plans, the NIP is overarching and strategic, both in the scope of tasks it contains and the planning process that it initiates for the U.S. Government. Other interagency strategic operational plans have a more focused functional or regional scope—such as the National Strategy to Combat Terrorist Travel—but follow the same process of planning, implementing, assessing, and adjusting.

At the more tactical end of the planning process are dynamic planning efforts, including those established to address emerging threat streams—for example what we have assessed to be the current heightened strategic threat window. For this reason, the White House directed NCTC to establish and lead an Interagency Task Force (ITF) to develop additional options and measures to increase intelligence collection and disrupt potential al-Qa'ida planning. Although led by NCTC, the ITF comprises a core group of representatives from the departments and agencies with the greatest responsibility for implementing new activities in the near term—including the Departments of Defense, State, Homeland Security and Justice.

Each week senior White House and Departmental officials review the actions proposed by the ITF, consider alternative options, and provide further direction on particular activities or measures recommended by the task force. Although I am unable to publicly describe specific actions taken by any single agency or department without undermining their effectiveness, I can report that the ITF has implemented a number of coordinated offensive and defensive measures designed to decrease the likelihood of a successful terrorist attack against the United States and our interests abroad. In addition, the ITF is continuously evaluating intelligence to recommend the most appropriate actions, assess

ongoing operations, and ensure that U.S. Government resources are aligned to most effectively address the threat.

After we have developed a plan to address a specific CT issue or challenge, and taken it through NSC's policy approval process, we move into the implementation phase. NCTC's role in this implementation process is not directive; as clearly delineated in the IRTPA, we do not tell agencies and departments how to do their jobs or when to execute specific actions. Instead, the legislation charges us with the "interagency coordination of operational activities." In practice this means monitoring the key elements of the plan to ensure execution by the relevant departments and agencies. It means working through the obstacles to implementation that inevitably arise. It means identifying the gaps in the plan that are only apparent when execution begins or when the enemy adapts to ongoing activities. Finally, it means highlighting resource issues so that we can match our limited resources to our most urgent CT priorities.

The strategic planning process is less than glamorous. However, as the former Director for Strategic Plans and Policy (DJ-5) for the Joint Staff, I believe it is absolutely critical to the long term success of our government as we prosecute the long war on terror. It is, in short, a revolutionary new way of doing business for the U.S. Government.

Throughout this process, all of our SOP efforts are designed to provide the context and the connective tissue to link the President's CT strategy with the operations and activities on the front lines of the War on Terror.

In closing, I would reiterate that we have come a long way in the last two years as a Center and in the last several years as a Community despite our continued challenges, six years after 9/11, I believe the United States is better prepared to fight this war than at any time in our history. Let me list seven reasons why I believe that.

First, our intelligence is better. Terrorists are clearly a difficult target, but our collection, analysis and production are significantly improved.

Second, we have made major strides in information sharing – in getting that intelligence to the people who need it.

Third, we have taken the fight to the enemy and achieved significant successes in the field. Thousands of terrorists have been taken off the field of battle and dozens of plots have been disrupted.

Fourth, we are attacking every element of the terrorist life cycle, including travel and finance.

Fifth, this is not only an American effort. We are working more closely and more effectively with a greater number of allies around the world to defeat the terrorists.

Sixth, and of special interest to this committee, we have taken significant steps to make the homeland a hostile place for terrorists to enter and operate.

Finally, through a new strategic planning effort, we are laying the groundwork to take the efforts already underway to a new level of integration and effectiveness.

All of this means we are safer than we were on September 11, 2001.

But we are not safe. Nor are we likely to be for a generation or more. We are in a long war, and we face an enemy that is adaptable, dangerous, and persistent and who always has a vote. While we have won many battles since 9/11, there are many battles yet to be fought and setbacks are certain to come along the way.

Thank you. This concludes my remarks.