BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
TTY: (202) 226–4410
http://science.house.gov

August 21, 2008

Mr. Edward Maquire
Inspector General
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Inspector General Maquire:

One of the key findings of the 9.11 Commission[1] that investigated the September 11, 2001 terrorist attacks was that the U.S. intelligence and law enforcement communities had failed to "connect the dots" and share vital terrorist intelligence that may have detected the 9.11 plot and possibly prevented those attacks. One of the commission's key recommendations was to unify all terrorist intelligence data from all government agencies under a National Counterterrorism Center. Without centralizing the collection, review and analysis of all of the government's terrorist intelligence information, the commission warned, "it is not possible to 'connect the dots.'"[2]

The National Counterterrorism Center (NCTC) was established in 2004 to coordinate government counterterrorism efforts and integrate the government's terrorism intelligence data. The NCTC "serves as the central and shared knowledge bank on terrorism information" and "establishes the information technology (IT) systems and architectures within the NCTC and between the NCTC and other agencies that enable access to, as well as integration, dissemination, and use of, terrorism information."[3] As part of its mission, the NCTC, which reports to the Office of the Director of National Intelligence (ODNI) maintains, updates and integrates all intelligence information from across the federal government regarding known or suspected terrorists.[4] This data is stored in a database called the Terrorist Identities Datamart Environment (TIDE) that is used to help compile the government's consolidated terrorist watchlist.[5]

---

[1] The official title of the 9.11 Commission is the National Commission on Terrorist Attacks Upon the United States. The commission's final report is accessible at: http://www.9-11commission.gov/.
[2] The 9.11 Commission Report, p. 408.
[3] National Counterterrorism Center: "What We Do;" http://www.nctc.gov/about_us/what_we_do.html.
[4] Homeland Security Presidential Directive/HSPD-6, "Integration and Use of Screening Information," September 16, 2003, available at: www.whitehouse.gov/news/releases/2003/09/print/20030916-5.html. This directive mandates that the Terrorist Threat Integration Center (TTIC), the predecessor to the NCTC, integrate and maintain all government terrorist intelligence information.
[5] "Terrorist Identities Datamart Environment (TIDE) Fact Sheet," National Counterterrorism Center, last updated February 2008, available at: http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf.

But, the Subcommittee has learned that the TIDE database is suffering from serious, long-standing technical problems. The Subcommittee has also learned that a critical NCTC initiative, named "Railhead," which is intended to replace TIDE with enhanced capabilities has suffered from severe technical troubles, poor contractor management and weak government oversight. As a result, potentially hundreds of millions of dollars have been wasted, delivery schedules have slipped, contractor employees have been laid off in order to restrain escalating costs, and the NCTC is now scrambling either to fix the technical troubles or possibly to abandon the program altogether. The end result is a current IT system used to identify terrorist threats that has been crippled by technical flaws and a new system that if actually deployed will leave our country more vulnerable than the existing yet flawed system in operation today.

Even if the Railhead program is abandoned, however, technical problems in the existing TIDE database will remain and must be examined and corrected. It is essential that the TIDE system properly process, review and include relevant terrorist intelligence data being provided to NCTC. The TIDE data forms the backbone of our efforts to perform counterterrorism analysis and to make critical assessments about the current and future terrorist threat. As the Central Intelligence Agency's (CIA) Chief Information Officer, Al Tarasiuk, said in a recent interview: "The thing that worries me the most is that we have buried somewhere, in some database, some piece of information that a person that might need access to doesn't have the access or the data is not available to them somehow."[6] Unfortunately, the Subcommittee understands that tens of thousands of potentially vital CIA messages flowing into NCTC have not been properly processed, reviewed or included in the TIDE database.

Given these technical problems, it is unclear if senior counterterrorism officials are confident that TIDE is appropriately gathering and maintaining all relevant terrorist intelligence data and operating effectively. The TIDE database, for instance, has reportedly crashed several times over the past few months delaying the delivery of updated terrorist intelligence data to the FBI's Terrorist Screening Center on numerous occasions. Fundamental design flaws in the database contribute to these problems.

The TIDE database does not conduct text based searches like popular search engines, such as Google, for instance. Instead, TIDE relies on Structured Query Language (SQL), a cumbersome and complex computer code that must utilize complicated sentence structures to query the TIDE database. Without a detailed index of the data stored in each table in TIDE, the SQL search engine is blindfolded, unable to locate or identify undocumented data. The current TIDE database is composed of data fields that are presented in 463 separate tables, 295 of which are undocumented.[7] As a result, critical terrorist intelligence in the TIDE system may not be searched at all.

---

[6] Thomas Wailgum, "Inside the CIA's extreme technology makeover, part 3," CIO (Chief Information Officer) Magazine, August 6, 2008, available at: http://www.cio.com/article/441688/Inside_the_CIA_s_Extreme_Technology_Makeover_Part_

[7] "Technical Exchange Meeting," Bahama IDP, RAILHEAD, July 16, 2007, unclassified.

The National Counterterrorism Center pulls terrorist intelligence data into the TIDE database "from more than 30 networks in an unprecedented effort to uncover and disrupt terrorist plots ...."[8] Maintaining and updating the data fed into TIDE from the CIA, NSA, Department of State, and other intelligence sources on a daily basis as well as ensuring that only qualified terrorist intelligence is available to the government's counterterrorist analysts is a growing concern. "The single biggest worry that I have is long-term quality control," Russell E. Travers, Deputy Director, Information Sharing and Knowledge Development at NCTC told The Washington Post last year.[9] There is no fool proof way to ensure that only good data gets into the TIDE database and unqualified data stays out. But the technical issues that hinder TIDE's ability to properly process, store and search the data it does have is a major concern.

Even worse, the incremental IT upgrades and projects currently being developed under the Railhead program may actually increase the technical problems and reduce capabilities to maintain, update, integrate, analyze and share the government's repository of terrorist intelligence. This situation threatens the ability of the NCTC to fulfill its critical counterterrorism mission. One NCTC information system, named NCTC Online or NOL, currently provides access to cable message traffic, Intelligence Community websites and data from 23 separate sources. But the new NOL system being developed under the Railhead program will *not* provide access to "any Intelligence Community websites or data sources."[10] This downgrade in the NOL's capabilities will prevent access to websites of the CIA, DIA, FBI and NSA and their data sources including Intelink and CIASource, for instance.[11] Assessments of other Railhead projects show they will also provide diminished search and analysis capabilities and increase potential technical risks.

Today, there are 546 unique baseline requirements regarding user interface applications on one current version of TIDE, for instance, known as TIDE Online (TOL), used by analysts outside of NCTC that permits them to search information about persons in TIDE.[12] Yet, the Railhead program's new version of TOL will include just 36 of the existing 546 user features in the current system,[13] significantly reducing its capabilities.

Software testing of portions of the new Railhead system point to other problems as well. In one instance, Railhead software passed 148 tasks, but did not complete 26 others and failed 42 tasks. In another test, one of the Railhead software applications passed 42 tasks, but failed 58 others. Among some of the specific problems with the new Railhead software: It failed to create reports from the TIDE data, it was unable to

---

[8] "The National Counterterrorism Center: United to Protect," video transcript, National Counterterrorism Center, available at: http://www.nctc.gov/docs/nctc-video-transcript.pdf.

[9] Karen DeYoung, "Terror Database Has Quadrupled In Four Yeats; U.S. Watch Lists Are Drawn From Massive Clearinghouse," The Washington Post, March 25, 2007, p. A1.

[10] "RAILHEAD: System Concept Definition (SCD), SCD NOL-J Gap Analysis," Final Version 1.0, submitted: 18 June 2008," SRI International, p. 8 and p. 25. (Hereafter: "RAILHEAD: NOL-J Gap Analysis.")

[11] "RAILHEAD: NOL-J Gap Analysis," p. 8.

[12] "RAILHEAD: System Concept Definition (SCD), SCD TOL Gap Analysis," Final Version 1.0, submitted: 18 June 2008," SRI International, p.11. (Hereafter: "RAILHEAD: TOL Gap Analysis.")

[13] "RAILHEAD: TOL Gap Analysis," p.11.

schedule delivery of reports on a periodic basis or trigger a report based on data criteria and the software was unable to conduct a search of saved reports, a critical ability for counterterrorism analysts. It also failed to find non-exact matches for key entities, such as a suspected terrorist's name. Incredibly, it also failed to demonstrate the ability to use basic Boolean search terms, such as AND, OR and NOT.[14]

Separately, nearly half of the 72 "Action Items" in the Railhead program are past due. As of June 2008, two items were behind schedule and 34 were past due.[15] In addition, of ten specific task orders on Railhead, five of them costing an estimated $92.9 million were described as being "Significantly off-plan."[16]

Some Railhead insiders allege that a significant portion of the estimated $500 million dollars spent on Railhead has been inappropriately used to renovate a building of one of the prime contractors, The Boeing Company, into a Sensitive Compartmentalized Information Facility (SCIF) in Herndon, Virginia. These individuals have also questioned the technical solutions endorsed by the government to replace the current TIDE database, the qualifications of some of the Boeing subcontractors and potential conflicts-of-interest between the program director of another key Railhead contractor, SRI International, and the government's Railhead program manager because of their alleged close personal ties. In short, documents obtained by the Subcommittee suggest that, despite hundreds of millions of dollars invested in Railhead and years of development, the government has little to show for its efforts.

The problems on the Railhead program appear to be depressingly similar to problems on other major government IT initiatives which have resulted in schedule delays, increased financial costs and ultimately failure on some projects. The Government Accountability Office's (GAO) latest review of the Office of Management and Budget's (OMB) effort to oversee federal investment in information technology (IT) programs found that 413 government IT projects totaling more than $25 billion in FY2008 alone were "poorly planned, poorly performing, or both."[17] Overall, the problems are not diminishing. The GAO analysis shows that the number of these problem plagued programs increased by 239 projects and $13 billion in FY2009. The number of IT programs on the OMB's Management Watch List increased from 31% of federal IT projects in FY2007 to 72% of federal IT projects in FY2009.

Like many of these programs, the flaws and failures on Railhead have been exacerbated by weak government oversight, poor contractor management and lack of contractor accountability for the program's performance. Turf battles among contractors, particularly between the design team and development team, have hampered the sharing of critical technical data that has impaired the success of the Railhead program. In

---

[14] "RAILHEAD: NOL-J Gap Analysis," p. 10.
[15] "RAILHEAD: Program Overview," Mark Stephenson, National Counterterrorism Center, June 6, 2008.
[16] "RAILHEAD: Business & Contracts," Joe Skowronski, National Counterterrorism Center, June 6, 2008.
[17] "Information Technology: OMB and Agencies Need to Improve Planning, Management, and Oversight of Projects Totaling Billions of Dollars," Government Accountability Office, Testimony by David A. Powner, Director, Information Technology and Management Issues, GAO-08-1051T, July 31, 2008.

addition, one list of Railhead staff from January 2008 identifies a virtual army of 814 private contract employees from dozens of companies involved in Railhead and only 48 government officials keeping tabs on this mammoth and critically important national security program. In fact, an estimated one dozen government slots on Railhead have been vacant for more than one year. A combination of these management problems and technical troubles seems to have doomed the Railhead program to failure.

I welcome the apparent increased attention and oversight the Railhead program has recently begun to receive in the past few weeks from the NCTC and ODNI. But for a program that has been held up by senior counterterrorism leaders[18] as one of their most promising initiatives that may help prevent future domestic terrorist attacks, these efforts appear to be too little, too late. I understand that there may be current efforts underway to close down Railhead completely. Regardless of those actions, I strongly encourage you to investigate and review the current and past management and oversight failures on the Railhead program that have led to the program's massive technical problems.

Although your investigation may involve reviewing classified data, I also strongly encourage you to issue an *unclassified* report on lessons learned that can help federal agencies and government program managers gain a better understanding of key management procedures and appropriate oversight reviews that can help ensure that other IT programs are carefully evaluated, appropriately managed and given the government oversight they both require and deserve in order to succeed. I encourage you to make recommendations that can help forestall or at least identify potential technical problems early on in a program's design and development phase, avoid contractor mismanagement in the future, and enhance government oversight of similar major IT programs that are critically important to the nation's national security, economy, health and safety.

I have attached my staff's more detailed memo on the Railhead program for your review. The memo also raises specific questions you may want to pursue. If you have any questions or need additional information, please have your staff contact Douglas Pasternak, Subcommittee professional staff member, at (202) 226-8892, or Dr. Dan Pearson, Subcommittee staff director, at (202) 225-4494.

Your assistance in this matter is greatly appreciated.

Sincerely,

Brad Miller
Chairman
Subcommittee on Investigations and Oversight

---

[18] Shaun Waterman, "A litmus test for U.S. information-sharing," United Press International (UPI), January 10, 2007.

cc: F. James Sensenbrenner Jr.
Ranking Member
Subcommittee on Investigations and Oversight

Bart Gordon
Chairman
House Committee on Science and Technology

David Obey
Chairman
House Committee on Appropriations

Silvestre Reyes
Chairman
House Permanent Select Committee on Intelligence