TO: Chairman Brad Miller
Subcommittee on Investigations and Oversight
Committee on Science and Technology

FROM: Subcommittee Staff

RE: Questions regarding technical flaws, poor government oversight and potential contractor mismanagement on the National Counterterrorism Center's RAILHEAD information technology development program

DATE: August 21, 2008

As numerous U.S. government investigations have revealed, most notably the National Commission on Terrorist Attacks Upon the United States[1], commonly referred to as the 9.11 Commission, one of the fundamental failures of the law enforcement and intelligence communities to prevent the September 11, 2001 terrorist attacks was the inability to "connect the dots" and share critical terrorist intelligence data between U.S. government agencies. As part of the 9.11 Commission's recommendations to help rectify those failures and help prevent any future terrorist attacks the U.S. government created the Office of the Director of National Intelligence (ODNI), run by the Director of National Intelligence (DNI). Under the ODNI a National Counterterrorism Center (NCTC) was also established, which "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."[2]

Among the NCTC's many functions is the maintenance and upkeep of the Terrorist Identities Datamart Environment (TIDE), the central repository of data on international terrorist identities within the United States Government,[3] described by the former Director of NCTC, Vice Admiral (Ret.) John Scott Redd, to a reporter as "the mother of all databases."[4] As the former director said: "Whether it comes from an operations cable from the CIA or a very sensitive SIGINT [signals intelligence intercept] from NSA, if there's a piece of derogatory information on a known or suspected terrorist, it goes in that [TIDE] database." Names, dates of birth, addresses and other key information is then pulled from the TIDE database and a "sensitive but unclassified" version of the data is sent to the Federal Bureau of Investigations (FBI's) Terrorist

---

[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] National Counterterrorism Center: "What We Do;" http://www.nctc.gov/about_us/what_we_do.html.
[3] "Terrorist Identities Datamart Environment – Fact Sheet," National Counterterrorism Center, http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf
[4] See journalist Ronald Kessler's two-part series on the National Counterterrorism Center on www.newsmax.com and his interview with Vice Admiral John Scott Redd, the former director of the National Counterterrorism Center. Ronald Kessler, "NCTC: Up to 70 Terrorist Plots Each Day," August 15, 2006.

Screening Center. That information on known or suspected international terrorists is then combined with FBI information on known or suspected domestic terrorists into the Terrorist Screening Database (TSDB) in order to form the consolidated terrorist watch list. This watch list in turn is used to generate the Federal Aviation Administration's No Fly List, and many other intelligence, border security and law enforcement watch lists.

Last year, the current director of NCTC, Michael Leiter, described the counterterrorism center as "the exemplar of all source, integrated analysis. Our analysts have access to all available CT [counterterrorism] information through dozens of networks and databases," he said. "We focus on everything from threat warning to strategic analysis, both foreign and domestic; and, we serve a broad customer base, including the President, Departments and Agencies, and the Congress."[5] Among the largest and most expensive programs currently being funded by the ODNI is a program at the National Counterterrorism Center to improve and replace its current information technology systems, including the TIDE database, in order to enhance information sharing among federal agencies and improve access to counterterrorism intelligence data collected from more than 30 separate government networks that feed data into NCTC.

But the Subcommittee has learned that the program, named "Railhead," whose goal is to develop and deploy information technologies that enable and improve the sharing, fusing and analysis of terrorist intelligence data across government agencies, may actually hinder and handicap the U.S. government's ability to share data. The Railhead program may actually degrade the ability to provide intelligence data for use in the consolidated terrorist watch list at the FBI's Terrorist Screening Center. It may cripple NCTC's ability to share critical intelligence among U.S. government agencies. It will also potentially jeopardize the ability to provide vital search functions by counterterrorism analysts. Documentation obtained by the Subcommittee points to a host of technical problems on Railhead, potential contractor mismanagement, contractor disputes, agency turf battles, poor government oversight and schedule delays that have hindered and hampered legitimate information sharing efforts on the program, have resulted in the potential waste of hundreds of millions of taxpayer dollars and placed the government's key counterterrorism information sharing initiative in jeopardy of failing.

Despite that, the Railhead program has been touted in the press by Maj. Gen. (Ret.) Dale Meyerrose, the Associate Director of National Intelligence and Chief Information Officer of the ODNI as a model of how to effectively develop counterterrorism information sharing technologies.[6] The current director of NCTC, Michael Leiter, has also described Railhead in Congressional briefings as a means to make disparate terrorist intelligence information "integrated and accessible" in order to improve discovery of terrorist information and improve the "ease and span of access" to

---

[5] Statement for the Record By Edward Gistaro, National Intelligence Officer on Transnational Threats and Michael Leiter, Principal Deputy Director, National Counterterrorism Center to the House Permanent Select Committee on Intelligence and the House Armed Services Committee, 25 July 2007. Available at; http://www.dni.gov/testimonies/20070725_testimony.pdf.

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

this information.[7] Last year, Leiter, then the deputy director of NCTC who was confirmed as the director of NCTC in July 2008, told Congress that "NCTC has been working closely with the DDNI/C [Deputy Director of National Intelligence for Collection (DDNI/C)] and [Intelligence] Community collectors to ensure efforts are appropriately focused on any and all lead data associated with plots directed against the West, and specifically the U.S. Homeland."[8] But technical problems on the current TIDE database appear to be hindering those efforts, and its successor – Railhead – is on the verge of collapse.

The original TIDE database, built by Lockheed Martin, replaced the Department of State's TIPOFF database, designed and built by The Analysis Corporation[9], in the wake of the 9.11 terrorist attacks to automate the terrorist watch list. The TIDE database was built in Oracle as a relational database management system (RDBMS). This original database, however, suffers from basic design, management and maintenance inefficiencies and problems. For instance, only about 60% of the data, including names and addresses, mentioned in CIA cables provided to NCTC are actually extracted from these messages and placed into the TIDE database.[10]

The TIDE database has evolved overtime as both contractors and government employees have attempted to expand and enhance the database to improve their own use of the system. But none of them appear to have taken into account the overall design or engineering architecture of the entire system. As a result, there are now dozens of tables or categories for identical fields of information making the ability to search or locate key data inefficient, ineffective and more time consuming and difficult than necessary.

In addition, the TIDE database relies on Structured Query Language (SQL), a cumbersome computer code that must utilize complicated sentence structures to query the tables, rows and columns that encompass the TIDE database. Without proper documentation on whether a table contains information on names, addresses, vehicles, license plates or an individual's nationality, for instance, analysts have no valid mechanism to conduct a search of these "undocumented" tables.

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

---

[7] "NCTC/Mission Systems: Railhead Program Briefing," National Counterterrorism Center, Unclassified/FOUO, April 11, 2008. This briefing presentation was reportedly presented by NCTC Director, Michael Leiter and Dirk Rankin, the NCTC program manager for Railhead to staff of the House Appropriations Committee.

[8] Statement for the Record By Edward Gistaro, National Intelligence Officer on Transnational Threats and Michael Leiter, Principal Deputy Director, National Counterterrorism Center to the House Permanent Select Committee on Intelligence and the House Armed Services Committee, 25 July 2007. Available at: http://www.dni.gov/testimonies/20070725_testimony.pdf.

[9] "About TAC: History," The Analysis Corporation (TAC), available at: www.theanalysiscorp.com/content/About/1-History.aspx

[10] "Internal Users Focus Group," Meeting Minutes, RAILHEAD, May 12, 2008.

which are undocumented, according to one internal Railhead document.[11] As a result, critical terrorist intelligence in the TIDE system may not be searched at all. "Existing TIDE data model is complex, undocumented, and brittle," the document notes, "which poses significant risk to RLSI [Railhead Lead System Integrator[12]] data migration and modeling."

"Pocket liter," for instance, the scraps of information obtained when law enforcement, military or other officials empty a suspect's pockets, including phone numbers, addresses or credit card information, is contained in 23 separate tables in TIDE, rather than one single uniform table. But as problematic as the current TIDE system is, counterterrorism analysts may lose access to key data if the new Railhead system comes on line as planned at the end of 2008. "Specifically, users will no longer have access to data that will not be migrated [to the new system], such as pocket litter and border summaries," another recent Railhead document warns.[13] In fact, the new Railhead systems that NCTC hopes will replace the current TIDE database by early next year may not provide critical search, access, sharing and other vital functions the current system *does* currently provide.

The Railhead program was developed in order to improve, enable and enhance the ability to share and analyze government terrorist intelligence related data among and between federal agencies and government counterterrorism analysts. The program is based on two separate information technology contracts. The System Concept Definition (SCD) contract is the design portion of the Railhead program, which is being run by SRI International and various subcontractors, including SRA International and Bearing Point.[14] The Lead System Integrator (LSI) portion of the Railhead program is intended to develop, operate and maintain the overall Railhead program and its specific sub-projects. The primary contractor for the LSI portion of the Railhead program is the Boeing Company's Space and Intelligence Systems (S&IS) Mission Systems division.[15] Some of the key Boeing subcontractors are very young companies, including Solutions Made Simple, Inc. (SMSi)[16] and Kestrel Enterprises Inc.[17] both founded in 2002 and Mark Logic Corporation[18], a California-based company established in 2004.

Mark Logic is a provider of an XML content platform. Extensible Markup Language or XML is a computer language whose primary purpose is to help share structured data among information systems. According to the company's web-site, "The company's flagship product, MarkLogic Server, includes a unique set of capabilities to store, aggregate, enrich, search, navigate and dynamically deliver content." But there are

---

[11] "Technical Exchange Meeting," Bahama IDP, RAILHEAD, Monday, 16 July, 2007," unclassified.
[12] The Railhead Lead System Integrator (RLSI) refers to The Boeing Company and its subcontractors on the NCTC's Railhead program.
[13] "RAILHEAD: System Concept Definition (SCD), SCD NOL-J Gap Analysis," Final Version 1.0, submitted: 18 June 2008," SRI International.
[14] http://www.sri.com/about/
[15] http://sismissionsystems.boeing.com/aboutus/index.cfm
[16] http://www.sms-fed.com/
[17] http://www.kestrelei.com/
[18] http://www.marklogic.com/

critics who have warned against using XML for storing data, because it can significantly increase the file size and slow down transmission time, for instance.[19]

The SCD Railhead design team has expressed serious concerns about the viability of using an XML platform to replace TIDE. In a recent e-mail to Dirk Rankin, the government's Railhead Program Manager, Joe Strigle, the SRI program director on Railhead wrote that based on his "understanding of the storage requirements, performance requirements (servers required), and the complexity of implementing data relationship changes" that the "SCD remains concerned about the viability of the Mark Logic solution."[20] The Railhead design team said they were concerned that these risks would result in major schedule and cost overruns. "My biggest concern," wrote Strigle, "is that we get much farther down this path and get a big surprise at the end. Unless MarkLogic has done something different than their own documentation suggests this looks like a serious program risk," warned Strigle.

The SCD design team had originally recommended replacing the legacy TIDE database and legacy TIDE On-Line (TOL) with a relational database based on Oracle. But Boeing "proposed a different approach, i.e., to combine TIDE and TOL in an XML database."[21] That proposal was accepted by Railhead government program managers and is currently underway. The current TIDE database is built on an Oracle 10.1 platform, a Relational Database Management System (RDBMS) that offers the ability to create, read, update, and delete specific tables or data. It can also easily transfer data from one relational database to another. "[A]ll databases with which TIDE interfaces are based upon the relational model," according to a SRI risk mitigation paper.[22] But if the TIDE database is converted into an XML platform, the paper says, "unique custom [computer] code" may be "needed for each interface." Currently the TIDE database interfaces with more than 30 separate data networks.[23] "A significant amount of adapter code is being written to support the conversion from the existing relational data model to the XML schema," the paper added. "This limits compatibility with other COTS [commercial off the shelf software], and it increases O&M [Operations & Maintenance] costs, which is contrary to the objectives for Railhead," the paper warned.

A separate e-mail to Railhead Program Manager, Dirk Rankin, from a Computer Science Corporation (CSC) contractor informed him that one of the lead managers of the existing TIDE database had voiced concerns about the Mark Logic approach as far back as August 2007, "primarily because it is a much more tightly coupled solution that can lead to integration issues with other databases that new TIDE will probably need to work with," the CSC employee wrote. "He also indicated that this is similar to the problems

---

[19] Craig S. Mullins, "DBAs! You Should Fear XML!," The Data Administration Newsletter, April 1, 2003, available here: http://www.tdan.com/print/5065

[20] E-mail from Joe Strigle, SRI International, to Dirk Rankin, National Counterterrorism Center, Subject: Mark Logic Issues, June 24, 2008.

[21] "TIDE and TIDE Online (TOL): Risks and Risk Mitigation Strategy," SRI International, June 25, 2008.

[22] "TIDE and TIDE Online (TOL): Risks and Risk Mitigation Strategy," SRI International, June 25, 2008.

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

that befell the original TIDE design, which caused it to experience significant operational availability issues and necessitated a lot of rework to get it to a more stable state."[24]

Rankin responded by telling his deputy and NCTC's Chief of Architecture and Engineering to "elevate this issue as a top program technical risk." Rankin also asked to see the documentation that led to the selection of the MarkLogic product back in 2007, "if nothing else other than to establish the context within which this product selection was made," wrote Rankin. He also said he wanted NCTC's Architecture and Engineering to "recommend a set of alternatives for escaping the implications of a ML [MarkLogic] based design if ML turns out to be a dead-end, suboptimal solution for the Program."

Last December, Rankin laid out a set of requirements for the Railhead program in an internal NCTC web-blog, which was titled: "RAILHEAD: NCTC Chiefs of Staff Requirements Statements."[25] He also explained his hopes for the new Railhead information technology architecture and the importance of these planned changes for NCTC counterterrorism analysts and others. "NCTC users will be able to run complex queries against the data, tailor and generate reports, and create visual displays of the data in multiple media formats," Rankin promised. Yet a recent "gap analysis" by SRI International of what the new Railhead systems will *actually* provide is much less optimistic.[26] "The ability to search e-mails and discussion threads, and the ability to search for images and attachments will be absent," the report found. "Advanced search capabilities such as selecting a timeframe for FININTEL [Finished Intelligence] searches and allowing Boolean keyword searches of results will also be absent." The report concluded: "Without these major functions, the system will not fulfill its information sharing mission for the counterterrorism community."

The December Rankin memo also said the ability to conduct a "federated search" of other agencies' data would be incorporated into the new Railhead system. "At the present time," Rankin wrote, "the cross domain search capability is targeted to include terrorism related information in the following databases and sets available to NCTC: Hercules, Trident, Investigative Data Warehouse, Proton, ICREACH, ION, PISCES, TIDE, EMS and TASS. In addition, the capability to add other DoD and Homeland Security databases associated with terrorism operations should also be planned and supported, such as the Refugee and Asylum Processing Database, JIANT, and the Central Index System." Yet, the SRI International review found that "other than the receipt of cables, the new system will not provide connectivity to any Intelligence Community websites or data sources." This includes access to websites of the CIA, DIA, FBI and NSA, for instance, and databases including, Intelink and CIASource.

---

[24] E-mail from Gregory L. Point, Computer Sciences Corporation, to Dirk Rankin, National Counterterrorism Center, June 26, 2008.

[25] "RAILHEAD: NCTC Chiefs of Staff Requirements Statements," posted by Dirk Rankin, December 18, 2007.

[26] "RAILHEAD: System Concept Definition (SCD), SCD NOL-J Gap Analysis," Final Version 1.0, submitted: 18 June 2008," SRI International.

Significantly, the planned Railhead system was found to have major security shortfalls. Again, Rankin wrote, "the system needs to be compliant with other community systems (like DNI's Library of National Intelligence or CIA's CAPNet2.0) that will allow those systems to pull directly from NOL or for users on NOL to directly access and retrieve information from them." Yet, the SRI International review found the new Railhead system did not have critical record auditing, intrusion and abuse detection functions. "The system will not meet all security and auditing requirements," the SRI report found. "It will not have the capability to produce audit logs, which can be utilized for near-real-time intrusion detection. The application will not conform to ODNI classification standards for posted documents and webpages."

Despite all these problems, the Railhead program is the overarching program that will produce major upgrades to two primary NCTC information systems. One is called NCTC Online (NOL) that enables the U.S. government's counterterrorism community to post, manage and access finished intelligence products, raw cable messages and other relevant data in a classified environment. The other system is called TIDE Online (TOL) which is a "sensitive but unclassified" read-only version of the data in the TIDE database that is provided to counterterrorism analysts across the U.S. government.

Both of the Railhead versions of these systems have experienced significant technical troubles and are clearly marred by their inability to function effectively and provide the government's counterterrorism community with the tools they require. One recent internal Railhead e-mail described an assessment of the new NOL system by an employee of the Office of the Director of National Intelligence. "[F]eedback on the NOL demo from Wes Wilson suggested that it was an abysmal failure, and the search was woefully less than desired."[27] Railhead's success on the other major pillar of its information technology system has fared no better.

Today, for instance, there are 546 unique baseline requirements regarding user interface applications on the current TOL system, which permits analysts outside of NCTC to search information about persons in TIDE.[28] Yet, the Railhead program's new version of TOL will include just 36 of the existing 546 user features in the current system,[29] significantly reducing its capabilities.

Software testing of portions of the new Railhead system point to other problems as well. Many of the incremental development computer upgrades on the Railhead program have been tested through Hewlett Packard's Quality Center (HPQC) which "manages and governs quality processes and automates software testing," according to a HPQC brochure.[30] The testing center "helps you make sure that every dollar invested in IT, every resource allocated, and every application in development or production meets

---

[27] Internal RAILHEAD E-mail from William Ham, SRI International to John Lovegrove, SRA, et. al., Subject: RE: Sequence of TIDE and NOL retirement IDPs, June 13, 2008.

[28] "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.")

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

[30] Hewlett Packard Quality Center Brochure, available here: http://welcome.hp.com/country/us/en/prodserv/software.html.

your business goals," the brochure says. "It offers a seamless, consistent and repeatable process for all stages of application quality management—from gathering requirements, to planning and scheduling tests, analyzing results, and managing defects and issues."

What did these tests reveal on the Railhead software that it tested? 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 software: It failed to create reports from the TIDE data, it was unable to 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.[31]

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.[32] In addition, of ten specific task orders on Railhead five of them worth an estimated $92.9 million were described as being "Significantly off-plan."[33]

Last year, the Railhead program was touted in the press by Maj. Gen. (Ret.) Dale Meyerrose, Associate Director of National Intelligence and Chief Information Officer of the ODNI as a model of how to effectively develop counterterrorism information sharing technologies.[34] The NCTC's current director, Michael Leiter also testified before Congress and cited TIDE as a major improvement in the government's counterterrorism initiatives. "The establishment and continued refinement of TIDE represents a major accomplishment in our CT [counterterrorism] efforts," Leiter said. "Before 9/11, the US lacked a single database of all known and suspected international terrorists, and our reliance on multiple watchlists, maintained by separate departments, presented a major vulnerability," he said.[35] On April 11, 2008, Leiter, who was sworn is as Director of NCTC on June 12, 2008, provided a briefing on Railhead to congressional staff from the House Committee on Appropriations. According to his briefing slides, Leiter said, that the Next Generation NOL would provide "improved search, content management and support for Top Secret CT [Counter Terrorism] Community." His slides also said that the Next Generation TIDE would provide "increased automation, improved search and reporting."[36]

---

[31] "RAILHEAD: NOL-J Gap Analysis," p. 10.

[32] "RAILHEAD: Program Overview," Mark Stephenson, National Counterterrorism Center, June 6, 2008.

[33] "RAILHEAD: Business & Contracts," Joe Skowronski, National Counterterrorism Center, June 6, 2008.

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

[35] Statement for the Record By Edward Gistaro, National Intelligence Officer on Transnational Threats And Michael Leiter, Principal Deputy Director, National Counterterrorism Center to the House Permanent Select Committee on Intelligence and the House Armed Services Committee, 25 July 2007. Available here; www.dni.gov/testimonies/20070725_testimony.pdf.

[36] NCTC/Mission Systems, Railhead Program Briefing, 11 April 2008, Unclassified/FOUO.

Other officials in the Office of the Director of National Intelligence, including the director himself have also specifically pointed to TIDE and NCTC Online as hallmarks of the government's information sharing accomplishments. Last February, the Director of National Intelligence, J. M. McConnell and his Chief Information Officer, Dale Meyerrose, issued a report on "Information Sharing Strategy" in the U.S. Intelligence Community.[37] The report emphasized that "time is of the essence" in improving information sharing among intelligence agencies and said: "The tragic events of September 11, 2001, demonstrated that the United States needed greater integration across the Intelligence Community and improved information sharing to respond to evolving threats and to support new homeland security customers." Furthermore, it boasted, "NCTC has developed innovative solutions, including NCTC Online and Terrorist Identities Datamart Environment [TIDE], to increase information sharing and collaboration in support of the counterterrorism mission."

But like so many other government programs, Railhead seems to have suffered from a critical and crippling lack of government oversight. An estimated one dozen government slots on Railhead, for instance, have been vacant for more than one year. As a result of these appalling management shortcomings and severe technical flaws, Railhead seems headed on a path that may actually *diminish,* not improve, the government's counterterrorism capabilities. In addition, hundreds of millions of dollars have already been spent on a system that appears to have been doomed to failure from the start. It is unclear if NCTC Director Leiter or other government officials were fully aware of the significant technical troubles the Railhead program had encountered at the time of their public statements to Congress and the public. But, at the time of their statements the Railhead program was imploding internally.

The abysmal technical performance of Railhead and the rosy comments by these officials raise fundamental questions about appropriate government and congressional oversight. Either the contractors were not fully apprising the government of the problems on the program; government program managers did not realize the seriousness or potential consequences of the problems; or senior officials at NCTC and ODNI did not share these problems and concerns with Congress, at least in any public forum. Poor technical planning, contractor malfeasance or weak government oversight, however, are not reasons to shield these problems and the potential waste of hundreds of millions of dollars in taxpayer funding from public scrutiny. It is also not an excuse to simply bury these issues behind a cloak of secrecy in order to escape responsibility for these failures.

As the 9.11 Commission concluded: "The challenge of technology ... is a daunting one. It is expensive, sometimes fails, and often can create problems as well as solve them. ... Despite the problems that technology creates, Americans' love affair with it leads them to also regard it as the solution."[38] Technology is essential to our national

---

[37] "United States Intelligence Community: Information Sharing Strategy," Office of the Director of National Intelligence, February 22, 2008. Available at: www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf

[38] The 9/11 Commission Report, p. 88. The full report of The National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission) is accessible at: http://www.9-11commission.gov/.

security and routinely provides solutions to daunting problems. But without proper and continuous oversight of Railhead and other innovative and challenging initiatives these programs will be technically and financially doomed to failure from the start.

The Subcommittee staff believes that it is critically important that there is a full accounting for the management failures, technical problems and ultimately financial waste encountered on the Railhead program. These issues should be thoroughly investigated by the Inspector General of the Office of the Director of National Intelligence or another appropriate entity. Among the key questions they should ask:

1. Was the basic design for TIDE On-Line and NCTC On-Line, based on the Mark Logic XML platform, a sound technical approach?
   a. Who was responsible for making these decisions and what technical documents did they use to justify this decision?
   b. Does NCTC still believe that basing the new TIDE database on the Mark Logic XML platform is managerially sound, technically appropriate and financially wise?

2. Were the prime contractors and the subcontractors involved in Railhead on both the LSI and SCD teams vetted and accessed appropriately?

3. The government's Railhead program manager, Dirk Rankin, is reportedly a close personnel friend of the SRI International Railhead program manager, Earl D. Lybarger. Did that relationship adversely influence the letting of the contract to SRI International and did it play any role in the technical, management or other problems on Railhead?

4. Congress appropriated funds for the construction of a new building to house the National Counterterrorism Center and its estimated 400 employees from the nation's 16 separate intelligence agencies. Yet, some individuals involved in the Railhead program have raised questions about the government's apparent use of nearly $200 million to retrofit one of Boeing's office buildings to house some of the 800 contractors on the Railhead program.
   a. Did the government actually fund the construction costs associated with the retrofit of the Boeing building in Herndon, Virginia?
   b. Was it appropriate and necessary for the government to spend nearly $200 million to turn Boeing's office space into a Special Compartmented Information Facility (SCIF)?
   c. What are the contractual arrangements regarding the government's apparent lease of office space in this Boeing building?
   d. How much is the U.S. government paying for this office space?
   e. Was the government's alleged arrangement to fund the retrofitting of the Boeing building and then lease it from Boeing appropriate and justified?

f. What are the financial implications for both Boeing and the U.S. government of these arrangements if the Railhead program is cancelled or drastically reduced in size and scope?

5. Before replacement systems for TIDE are developed, it is critically important to conduct a thorough technical configuration audit of the current TIDE database to determine where current processing, searching, or other problems currently exist and how they may be corrected to increase the efficiency and effectiveness of the current TIDE system and any future upgraded systems.

6. What are the key lessons learned from the Railhead program?

   a. Are there specific recommendations that can enhance the government's overall ability to properly and thoroughly select and vet major IT contractors and the design and development plans of IT projects *before* problems emerge and hundreds of millions of dollars in government resources are squandered?

   b. According to one document, as of January 2008, the Railhead program included a total of 862 employees, including 48 government officials, 16 employees of MITRE, the government's federally funded research and development center (FFRDC) providing oversight support of Railhead, and 798 other contractors. Was this a sufficient pool of government personnel, with the appropriate expertise, to provide the necessary management and oversight of the Railhead program? Are there general recommendations that can be made regarding the appropriate mix of government personnel on future IT programs?