U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 3, 2006

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on July 27, 2005. The subject of the Committee's hearing was oversight of the Federal Bureau of Investigation.

We hope that this information is helpful to you. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Responses of the Federal Bureau of Investigation Based Upon the July 27, 2005 Hearing Before the Senate Committee on the Judiciary Regarding FBI Oversight

Questions Posed by Senator Specter

1. Larry Johnson, a former counter-terrorism official at the State Department, said in a July 16, 2005 issue of the National Journal that the FBI is on its sixth counter-terrorism chief since 2001. "There is a rhetorical gap the size of the Grand Canyon, in which the Bush Administration on one hand insists that fighting terrorism is the No. 1 priority, and yet as far as personnel goes, it is treated as the last priority."

a. List the names of each of the FBI counter-terrorism chiefs, with their dates of service in this position and the reasons for their departure. Include as an attachment to this response all internal documents that set forth the reasons for the departure including, but not limited to, employment records. Provide a résumé, curriculum vitae or biography of each of the persons who held this position.

Response:

Following are the assignment histories of each Assistant Director (AD) of the FBI's Counterterrorism Division (CTD). Please note that before 11/21/1999, counterterrorism (CT) was part of the National Security Division, which became the Counterintelligence Division (CD) following an FBI reorganization (these assignments are referred to below as assignments to the CD).

Dale L. Watson
Entered on duty as a Special Agent (SA) on 2/12/78.
Assigned to Birmingham Division on 5/20/78.
Reassigned to New York on 10/19/82.
Reassigned to CD, FBI Headquarters (FBIHQ) on 1/6/85.
Promoted to Supervisory Special Agent (SSA), CD, on 1/19/86.
Reassigned to Washington Field Office (WFO) on 3/11/87.
Promoted to Unit Chief (UC) in the Criminal Investigative Division (CID) on 11/25/91.
Reassigned to CD UC on 4/23/92.
Promoted to Assistant Special Agent in Charge (ASAC), Kansas City Division, on 5/3/94.
Reassigned to CD as a GS-15 SSA on 9/1/96 and detailed to the National Security Agency.
Promoted to Section Chief (SC), CD, on 12/13/96.

Promoted to Deputy Assistant Director (DAD), CD, on 7/8/98.
Promoted to AD, CTD, on 12/14/99.
Promoted to Executive Assistant Director (EAD), CT/Counterintelligence (CI), on 12/2/01.
Retired on 9/30/02.

Pasquale J. D'Amuro
Entered on duty as an SA on 5/6/79.
Assigned to the New York Division on 8/22/79.
Promoted to SSA on 2/15/87.
Assigned as Assistant Inspector, Inspection Division, on 4/30/95.
Promoted to GS-15 SSA, CID, on 7/8/96.
Reassigned as ASAC-CT, New York Division, on 8/31/97.
Promoted to Associate SAC, New York Division, on 1/29/01.
Promoted to AD, CTD, on 1/29/02.
Promoted to EAD, CT/CI, on 11/14/02.
Reassigned as Assistant Director in Charge (ADIC), New York Division, on 8/4/03.
Retired on 3/31/05.

Larry A. Mefford
Entered on duty as an SA on 8/6/79.
Reassigned to Sacramento Division on 11/23/79.
Reassigned to Los Angeles Division on 9/15/80.
Reassigned to WFO on 12/21/86.
Reassigned to the Critical Incident Response Group on 9/27/87.
Promoted to SSA, CID, on 11/5/89.
Reassigned to Minneapolis Division on 4/6/92.
Reassigned to San Francisco Division as an SA on 7/9/95.
Promoted to SSA, San Francisco Division, on 5/11/97.
Promoted to ASAC, San Diego Division, on 9/27/98.
Promoted to Associate SAC, San Francisco Division, on 6/12/00.
Promoted to AD, Cyber Division (CyD), on 5/28/02.
Reassigned as AD, CTD, on 11/22/02.
Promoted to EAD, CT/CI, on 8/18/03.
Retired on 10/31/03.

John S. Pistole
Entered on duty as an SA on 9/18/83.
Assigned to Minneapolis Division on 1/6/84.
Reassigned to New York Division on 4/7/86.
Promoted to SSA, CID, on 11/30/90.

Reassigned to Indianapolis Division on 3/21/94.
Promoted to ASAC, Boston Division, on 7/4/99.
Promoted to Inspector on 7/23/01.
Promoted to DAD, CTD, on 6/3/02.
Promoted to AD, CTD, on 9/16/03.
Promoted to EAD, CT/CI, on 12/22/03.
Promoted to Deputy Director on 10/3/04 (current position).

Gary M. Bald
Entered on duty on 9/11/77 and assigned to the Criminal Justice Information Services (CJIS) Division as a fingerprint examiner.
Reassigned to the Laboratory Division as a physical science aid on 4/24/78.
Promoted to cryptanalyst on 10/23/78.
Became an SA on 4/19/81.
Assigned to Albany Division on 8/10/81.
Reassigned to Philadelphia Division on 3/31/84.
Promoted to SSA, Inspection Division, on 6/4/89.
Reassigned to Newark Division on 8/9/91.
Promoted to GS-15 Assistant Inspector, Inspection Division, on 4/16/95.
Reassigned as UC, CID, on 9/3/96.
Promoted to ASAC, Atlanta Division, on 12/2/96.
Reassigned as Inspector-in-Charge on 2/25/00.
Promoted to SAC, Baltimore Division, on 9/30/02.
Promoted to DAD, CTD, on 11/17/03.
Promoted to AD, CTD, on 3/4/04.
Promoted to EAD, CT/CI, on 11/2/04 (current position).

Willie T. Hulon
Entered on duty as an SA on 9/6/83.
Assigned to Mobile Division on 12/22/83.
Reassigned to Chicago Division on 1/28/86.
Reassigned to San Antonio Division on 4/11/88.
Promoted to SSA, San Antonio Division, on 10/20/91.
Reassigned to CID on 3/19/95.
Promoted to GS-15 Assistant Inspector, Inspection Division, on 2/4/96.
Reassigned as UC, CID, on 6/2/97.
Promoted to ASAC, St. Louis Division, on 3/9/98.
Promoted to Inspector on 11/3/00.
Promoted to Chief Inspector on 7/26/01.
Promoted to SAC, Detroit Division, on 12/3/02.
Promoted to DAD, CTD, on 6/7/04.
Promoted to AD, CTD, on 12/26/04 (current position).

b. Provide a statistical report of the number and percentage of FBI human resources assigned solely and entirely to the Counter-Terrorism Division of the FBI.

Response:

The response to this inquiry is classified and is, therefore, provided separately.

2. How much of the FBI's resources are dedicated to intelligence, as opposed to prosecutorial, work?

a. What percent of your human resources are assigned full-time to intelligence gathering as opposed to the prosecutorial support role?

Response:

Intelligence is integrated into all aspects of the FBI's law enforcement mission, and is both an investigative tool and a mission unto itself. Intelligence is also a key objective that is pursued during the prosecutorial phase of an investigation. For this reason, it is difficult to answer this question without a clear context. The resources devoted to intelligence as a mission in and of itself (as opposed to intelligence used and produced in the context of an investigative mission) fall, as an accounting matter, within the FBI's Intelligence Decision Unit (IDU). Of the positions included in the FBI's Fiscal Year (FY) 2005 Congressional appropriation (including the FY 2005 supplemental), 15.5 percent are included in the IDU. These positions include the staff assigned to the Directorate of Intelligence (DI) and personnel under the programmatic control of the EAD for Intelligence (EAD-I), as well as a pro rata share of operational, investigative, management, and other support personnel (such as finance, human resources, and legal personnel) who support the intelligence mission.

We stress, however, that no neat dividing lines distinguish intelligence from law enforcement activities. Intelligence is a core investigative tool, and a valuable product of the prosecutorial phase of an investigation.

b. What is the number of full-time equivalents (FTEs) in Intelligence?

Response:

The FBI's FY 2005 Congressional appropriation included 4,365 full-time equivalents in the IDU.

c. What percent of your monetary resources are used in intelligence?

Response:

16.5 percent of the FBI's FY 2005 Congressional appropriation (including the FY 2005 supplemental) is included in the IDU.

3. Director Mueller stated in a recent speech: "The development of the National Security Service ("NSS") is the next step in the evolution of our ability to protect the American public."

a. What plans, policies and strategies has FBI implemented toward this goal?

Response:

The FBI will submit its National Security Branch Implementation Plan to the President shortly. This Plan is being coordinated with the Office of the Director of National Intelligence (ODNI), and several issues must be resolved before submission. In response to the President's six specific instructions, the Plan provides statements of principle from which detailed implementation plans will be developed. As articulated in the Plan, the National Security Branch (NSB) will strengthen the FBI's existing capabilities in these areas by combining the CTD, CD, and DI into an integrated service that effectively leverages the assets and abilities of all three entities. The NSB will be headed by an EAD.

b. Set forth the process by which FBI and Director Negroponte will appoint the head of the NSS.

Response:

The President has directed that the head of the NSB be appointed with the concurrence of the Director of National Intelligence (DNI), and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directs that the Attorney General obtain the concurrence of the DNI before appointing an individual to the position of EAD for Intelligence or any successor position created through reorganization. Because the head of the NSB (the EAD-NSB) is the successor to the EAD-Intelligence position, the FBI Director forwarded to the Attorney General his recommendation for appointment to the position of EAD-NSB. Consistent with the IRTPA, the Attorney General sought the concurrence of the DNI before making the appointment.

The FBI Director recommended Gary M. Bald, EAD for CT/CI, for appointment as the EAD-NSB. This recommendation was approved by the Attorney General, and the DNI concurred in the appointment. The Deputy appointed to assist EAD Bald in directing the NSB is Philip Mudd from the Directorate of Operations at the Central Intelligence Agency (CIA).

4. Joint Terrorism Task Forces (JTTFs) were set up to coordinate counterterrorism activities between the FBI, state and local law enforcement agencies. The 9/11 Commission Staff Report no. 9 (pg. 10) states that most local and state law enforcement representatives to the JTTFs were simply liaisons and did not fill management or investigative positions.

a. Are there currently any non-FBI officials in management positions in any JTTFs?

Response:

At the discretion of the ADIC or SAC (while most Field Divisions are led by SACs, very large FBI Field Divisions are led by ADICs), participating agencies that have devoted significant numbers of employees or resources to a Joint Terrorism Task Force (JTTF) may assign supervisory personnel to handle administrative matters for their employees. Presently, the New York JTTF includes the largest number of management level non-FBI officials (a New York Police Department (NYPD) deputy chief, captains, lieutenants, and sergeants). These are not operational management positions, but are instead filled by personnel managers for the 115 NYPD employees assigned to the New York JTTF. Management-level officials are also assigned to many other JTTFs for the same purpose. In addition, each JTTF has an Executive Board that is chaired by the FBI's ADIC or SAC and is composed of senior federal, state, and local law enforcement officials who review the operations of the JTTF and provide input and recommendations as to the JTTF's investigative direction.

b. If not, why not?

Response:

For command and control purposes, the FBI ADIC or SAC is a JTTF's overall commander and is responsible for the operational and administrative matters directly associated with that Division's JTTF(s). The operational chain of command (in "top down" order) is as follows: ADIC (if applicable), SAC, ASAC, and SSA. Staffing issues are the responsibility of the FBI chain of command, while the SSA, as the JTTF Supervisor, supervises JTTF operational

activities. All JTTF investigations are opened and conducted in conformance with FBI policy.

c. If so, set forth the name, location and position of such non-FBI official.

Response:

Although many JTTFs include non-FBI members in management-level positions with respect to members of their organizations, none are in operational management positions. In the largest New York JTTF, as with other large JTTFs, the staff of each operational squad includes an NYPD sergeant who collaborates with the FBI squad supervisor regarding investigative decisions. This collaboration also occurs among more senior managers, where NYPD lieutenants, captains, and higher share decision making with FBI executive managers. This enhances investigative oversight, which contributes to a more effective CT effort. Ultimately, though, the FBI is responsible for ensuring investigations are conducted in accordance with all aspects of federal law, Attorney General Guidelines, and Department of Justice (DOJ) and FBI policy.

d. How many JTTFs exist today and how many FBI personnel are assigned full time to each JTTF?

Response:

Currently, the 103 JTTFs are staffed by a total of 3,714 full-time law enforcement officers, including 2,196 FBI SAs, 683 officers from other federal agencies, and 835 state and local law enforcement officers.

5. A July 19, 2005 *New Yorker* article entitled "*Defending the City*" describes the FBI agents assigned to an NYPD counterterrorism center as "young white men ... standing stiffly against a wall."

a. What kind of interaction do you expect from your agents detailed to local counterterrorism centers?

Response:

FBI personnel assigned to local or regional CT centers or to Regional Intelligence Centers (RICs) are expected to be fully engaged, along with other federal, state, and local agencies, in accomplishing the center's mission. FBI personnel are assigned to these centers to facilitate an unimpeded flow of information concerning terrorism threats and intelligence between the centers and the JTTFs,

which are the primary operational and investigative arms of the U.S. Government in the war on terrorism. Coordination between regional CT centers, RICs, the FBI's CTD, and other appropriate entities is accomplished through those assigned or detailed to the JTTFs and to Field Intelligence Groups (FIGs).

b. Does the FBI plan to make the efforts of municipal law enforcement agencies an integrated part of their counterterrorism operations, contrary to what is being reported?

Response:

The FBI currently incorporates the efforts of municipal, state, and other federal agencies in CT operations because it has found that success against terrorism is best achieved through cooperation among federal, state, and local law enforcement and public safety agencies. The FBI formed the JTTFs to maximize interagency cooperation and coordination and to create cohesive units capable of drawing on resources at all government levels in responding to terrorism threats. Currently, the 103 JTTFs are staffed by 3,714 full-time law enforcement officers (including 835 state and local law enforcement officers) and augmented by 1,355 part-time law enforcement officers, including 121 FBI SAs, 708 officers from other federal agencies, and 526 state and local law enforcement officers.

c. If so, what specific plans does the FBI have to more fully integrate their agents into these centers?

Response:

FBI ADICs and SACs are encouraged to interact with and participate in regional CT centers and RICs in their territories. While there may not be a regional CT center or RIC in every ADIC's or SAC's territory, all FBI field offices currently manage and operate FIGs, which serve as the central intelligence component of every FBI Field Office and perform the office's core intelligence functions. The primary mission of these FIGs, which are predominantly staffed by FBI intelligence analysts (IAs), is to provide direct operational and strategic analytical support to the JTTFs. The FIGs and JTTFs both have roles in ensuring that intelligence collected by the JTTF is properly and timely disseminated to intelligence customers.

d. Has anyone within FBI Headquarters investigated these assertions made in the *New Yorker* article and has any corrective action been taken?

Response:

While the FBI is aware of this article, no changes or adjustments to the FBI's operating procedures have been made as a direct result of the claims made in the article.

6. The FBI often seems reluctant to share pertinent information with local and state law enforcement agencies. The *New Yorker* article cites an instance in October 2001 when the White House was informed that a 10-kiloton nuclear weapon was being smuggled into New York City (p. 61). Mayor Giuliani and the NYPD were not informed of this threat. Today, the NYPD complains that while the flow of information has improved, integrated intelligence sharing does not yet occur. What is the FBI doing to actively improve the flow of terrorism information between the FBI and state and local law enforcement agencies?

Response:

The FBI takes such criticisms very seriously and is implementing a three-pronged strategy to improve the flow of information through policy, organization, and technology. The FBI shares classified intelligence and other sensitive FBI data with federal, state, and local law enforcement officials through a variety of means, including the JTTFs, which partner FBI personnel with investigators from federal, state, and local agencies and are important force multipliers in the fight against terrorism. Since 9/11/01, the FBI has increased the number of JTTFs from 35 to 103 nationwide and has established the National Joint Terrorism Task Force (NJTTF) at FBIHQ, staffed by representatives from 38 federal, state, and local agencies. The NJTTF's mission is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of CT operations. The FBI agrees that effective information flow is critical and will continue to create new avenues of communication among law enforcement and intelligence agencies to better fight the terrorist threat.

The FBI's policy is to share by rule and withhold by exception. For example, while the FBI is committed to ensuring that its most sensitive law enforcement and intelligence sources and methods are protected from unauthorized disclosure, this is accomplished by sanitizing documents containing this information and then disseminating the resulting unclassified documents, rather than by merely withholding the unsanitized documents. The FBI has created a senior-level policy group, the Information Sharing Policy Group (ISPG), to ensure the framework

exists to facilitate compliance with the emphasis on broad dissemination. The ISPG is co-chaired by the FBI's EAD-I and EAD-Administration, and brings together the FBI entities that generate and disseminate law enforcement information and intelligence. Since its establishment in February 2004, this body has provided authoritative FBI policy guidance for internal and external information sharing initiatives. Working in conjunction with the Chief Information Officer (CIO) and his Program Management Executive (PME), the ISPG integrates information technology initiatives with FBI mission objectives, policy guidance, and legal authorities.

The FBI has also made technological and organizational changes to improve the flow of terrorism information between the FBI and state and local law enforcement agencies. Through our National Information Sharing Strategy (NISS), the FBI is implementing new technological tools to facilitate the sharing of regional and national criminal data with law enforcement agencies. NISS has three components: National Data Exchange (N-DEx), Regional Data Exchange (R-DEx), and Law Enforcement Online (LEO). N-DEx is the first national information sharing service. It will collect and process crime data from all major FBI databases, including the National Crime Information Center (NCIC), and will combine and correlate data to permit "one-stop shopping." N-DEx will give users access to information that will assist them in detecting and preventing terrorist attacks, in linking cases, and in forming broader investigative partnerships. Currently, N-DEx is in the pilot phase of operations, with full capability anticipated in 2007.

As a complement to N-DEx, R-DEx will enable the FBI to share data, including documents from its investigative files, electronically across federal, state, and local boundaries, improving the ability to prevent terrorism and other crimes by supplying the tools for using information in new analytical ways. R-DEx will also dramatically reduce the time spent by analysts in routine data entry, collation, and manual data manipulation by providing integrated information for use by all law enforcement agencies and by facilitating the analysis of law enforcement information, including queries, associations, and linkages to automated reports. The first R-DEx regional systems are in St. Louis and Seattle.

LEO, the third NISS component, uses Web-based communications capabilities to permit the law enforcement community to exchange information, conduct online education programs, and participate in professional special interest and topically focused dialog. LEO, which has been operational since 1995 and presently serves more than 42,000 users, has secure connectivity to the Regional Information Sharing Systems network. FBI intelligence products are disseminated weekly through LEO to more than 17,000 law enforcement agencies, providing

information about terrorism, criminal, and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public. Enhancements have permitted LEO to serve as the primary channel for Sensitive But Unclassified communications with other federal, state, and local agencies. The FBI also uses LEO to share intelligence products with Homeland Security Information Network (HSIN) users; states and major urban areas use the secure HSIN to obtain real-time interactive connectivity with the Homeland Security Operations Center and to share information with other HSIN users at the Sensitive But Unclassified level.

In addition to these technological enhancements, the FBI has also made organizational changes to enhance coordination with state and local law enforcement authorities. Among these was the establishment, in April 2002, of the Office of Law Enforcement Coordination (OLEC). Headed by a former state police chief, OLEC is responsible for ensuring that relevant intelligence is shared, as appropriate, with state and local law enforcement. As outlined in the FBI's Intelligence Policy Manual, the DI also shares information with our partners in state and local law enforcement through Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments.

In September 2003, the FBI also established FIGs in all Field Divisions. FIGs centrally manage the intelligence production and dissemination in FBI field offices, ensuring that state, local, and tribal law enforcement partners receive all relevant intelligence to support their missions. Among the key initiatives in this area is the joint development of intelligence requirements, along with state, local, and tribal partners, that clearly convey to FIGs the needs of those partners. In addition, in August 2005 the FBI worked with the Global Intelligence Working Group Requirements Subcommittee to develop a standing set of intelligence requirements for the United States Intelligence Community (USIC) and state, local, and tribal law enforcement with respect to national security and criminal intelligence topics. Once approved by the Criminal Intelligence Coordinating Council, this document will serve as the principal guidance for intelligence sharing between the FBI and other law enforcement organizations.

For information concerning the role of the Terrorist Screening Center (TSC) in sharing this important information, please see the response to Question 46.

7. In recent articles in the *New York Times* and other news sources, municipal police chiefs from New York, Los Angeles, Washington, D.C., Chicago, and Las Vegas repeatedly cite the FBI's unwillingness to share raw intelligence on a regular basis with their departments that would allow them to focus on the immediate threats in their cities. Washington Metropolitan Police Chief Ramsey stated, "I don't need a threat assessment. I need to know what I can do to proactively strengthen the security of our transit system." Is the FBI willing to allow local police departments' regular and immediate access to raw intelligence that is related to counterterrorism efforts in their jurisdictions?

Response:

As indicated in response to Question 6, above, the FBI has taken affirmative steps to improve the quantity and quality of shared raw intelligence, and we will continue to seek ways of improving that process.

8. Municipal police chiefs across the U.S. are discussing the formation of a nation-wide municipal counterterrorism network to supplement the flow of information from the FBI and DHS. Much of the discussion of this network has centered on the NYPD model of stationing agents in overseas countries to gather instant information that the FBI and DHS deliver hours or days later.

a. Does the FBI support this effort by local law enforcement to create its own national counterterrorism network?

Response:

The FBI considers state, local, and tribal law enforcement to be core nodes in the national CT network. We believe it is essential that such a network be part of the larger U.S. Information Sharing Environment (ISE), which is established under the direction of the ISE program manager pursuant to section 1016 of the IRTPA. Information sharing is crucial in the war on terrorism, and the FBI works with and participates in many of the regional fusion centers and other information sharing ventures that have already been established to ensure both that information from the national level is shared with state, local, and tribal law enforcement and that information developed by local law enforcement agencies is disseminated and shared with the national CT community, as well as with our foreign allies under appropriate circumstances.

The FBI defers to the Department of State for a judgment concerning the extent to which independent activities of state, local, and tribal law enforcement networks overseas may complicate U.S. foreign policy.

b. Does the FBI view this movement towards a national municipal counterterrorism network as a failure in their intelligence dissemination network?

Response:

The FBI does not view this initiative as a failure, but instead as a vital part of the nation's ISE.

c. What plans does the FBI have to fix this perceived problem?

Response:

The FBI's strategy to improve the flow of information through policy, organization, and technology is articulated in response to Question 6, above.

9. The FBI's lack of promptly sharing important terrorist information is so well known, that CNN uses the fact that local police obtain information sooner from CNN than from the FBI or DHS as a marketing tool in a prime-time commercial quoting local law enforcement that they receive their first information on terrorist activity from CNN.

a. Provide any written internal memoranda referring to this commercial and any written or oral response made by any FBI personnel to CNN.

Response:

We are aware of neither written internal memoranda referring to the commercial nor written response to CNN. We are also not aware of any oral discussions between the FBI and CNN regarding the commercial.

b. Provide a copy of any written communication and a written summary of any oral communication with any local law enforcement agents concerning this commercial.

Response:

Both oral and written communications with local law enforcement officials are frequent and wide ranging. While no such communications regarding the CNN commercial have come to the attention of senior FBI officials, we have no way of knowing whether informal communication on this topic has occurred.

10. The creation of the Information Sharing Environment ("ISE") has been described by some as marginalizing the responsibilities of the Department of Homeland Security by giving the information-sharing responsibilities of the federal government to a new agency.

a. How does FBI expect to interact with the ISE and what, if any, does FBI see as the role of the Department of Homeland Security in terrorist information sharing?

Response:

The FBI does not view the creation of the ISE as marginalizing the responsibility of any federal agency, including the Department of Homeland Security (DHS), and believes DHS's information-sharing role is defined in the Homeland Security Act of 2002. The ISE, specifically the ISE program manager, will establish information sharing technical standards and policies. The day-to-day sharing of content will occur in consonance with these standards, but will be accomplished by the individual agencies that comprise the U.S. CT network. The FBI expects to play a significant role in the ISE, including through the information sharing strategies discussed in response to Question 6, above, and will adjust its technical standards and policies to conform with those of the ISE.

Through the DI, the FBI has established FIGs in all field offices to ensure that terrorism intelligence needed by other agencies is extracted from investigative reports and disseminated to those agencies. This dissemination occurs at all levels of classification through direct message traffic and Web-based networks classified at the Top Secret-SCI level, the Secret level, the Sensitive But Unclassified level, and the Unclassified level. All FBI systems, networks, and communications channels will become part of the national ISE under the framework being developed by the ISE program manager, and the FBI is committed to using this framework to share as much terrorism information as possible. This commitment is reflected in the issuance of an Intelligence Policy Manual that provides specific guidance and emphasizes techniques to assist analysts in writing for dissemination.

The FBI does, however, remain committed to enforcing access controls to protect its most sensitive law enforcement and intelligence sources and methods from unauthorized disclosure in appropriate circumstances (such as when unauthorized disclosure would present a grave risk of compromise to the FBI's ability to obtain information about difficult collection targets). To maintain such protection, information may be disseminated in sanitized or declassified versions that are more easily used and shared by recipients.

b. How many employees does FBI plan on providing to ISE as "detailees?" If any, when and who will FBI provide?

Response:

The FBI is working with DOJ, the DNI, and the ISE program manager to determine the appropriate number of detailees, as well as their skill mix.

c. What other resources does FBI expect to provide to ISE and when?

Response:

Both DOJ and the FBI are prepared to offer any and all of our information technology and content to the ISE program manager, and are working with the program manager to ensure the appropriate integration of those resources into the ISE.

11. The FBI has in the past three years spent over $170 million dollars on the Virtual Case File system (VCF), only to recently inform the American people that all of their tax dollars were spent with nothing to show. Now the FBI has announced the all new Sentinel program as the system to fix all of their programs.

a. What specifically will happen that will ensure that Sentinel will not be another multi-million dollar fiasco?

Response:

As the FBI advised during the hearing, we recognize that the development of Virtual Case File (VCF) suffered from inadequate managerial control and changing technical requirements. Using a disciplined programmatic approach in Sentinel's development will allow us to leverage the lessons learned from that effort.

Among other things, this programmatic approach has led to the development of a new Life Cycle Management Directive (LCMD), which specifies numerous criteria for passage through strict control gates. Each step of the process is approved by an appropriate Information Technology (IT) governing board, as outlined in the LCMD, before the program can progress to the next step. This process is discussed further in response to Question 11e, below. Several other key factors will also contribute to the success of the Sentinel program.

- The assignment of dedicated, experienced program oversight personnel.

• Early formation of processing teams comprised of both government and contractor representatives.

• Rigorous application of Earned Value Management System (EVMS) controls (discussed in response to Question 11e, below).

• Award of the contract to a "best value" contractor – one with dedicated, experienced personnel and a proven track record.

• A disciplined award-fee contract process.

• A rigorous "change control" process to reduce technical requirement revisions.

In addition, the following efforts should significantly improve the efficiency and effectiveness of the Sentinel development process.

• Commercial off-the-shelf software will be used whenever possible to decrease development and maintenance expenses, time, and risk.

• The use of a modular, loosely coupled architecture will allow the easy replacement of components. A failure of one component will not cause the whole system to fail, which will reduce overall program risk. If necessary, individual commercial products can be quickly and easily replaced with other comparable products with minimal impact on the whole system. This modular design will also facilitate component upgrades and replacements as newer versions evolve.

• The flexible architecture will allow for rapid re-configuration if the FBI's business needs change.

• The use of prototypes of key Sentinel components (workflow, portals, and security managers) will permit the identification of potential integration issues before they would be encountered through a fully deployed Sentinel program. The use of these prototypes will also allow early user feedback, reducing the risk that Sentinel will not meet users' needs. Permitting operational users access to the prototypes before Sentinel is fully developed and deployed will also provide early operational benefits.

b. Provide copies of FBI Request for Proposals and any responses thereto regarding the Sentinel program.

Response:

The Sentinel Statement of Work is attached (Enclosure A).

Responses to the RFP constitute "source selection information" as defined by 41 U.S.C. § 423(f)(2), release of which is generally prohibited by law (41 U.S.C. § 423(a)). Because the disclosure of this information would jeopardize the integrity of the procurement process, and because information from vendors is proprietary to them and not the Government's information, we decline to disclose those responses.

c. What is the FBI budget for this new system?

Response:

The FBI has developed a cost estimate to be used for budgetary purposes, but revealing it would alert potential contractors to the government's expectations regarding contract price, which would compromise the ability of the source selection process to identify the lowest responsive, responsible bidder. The FBI will have a final cost estimate when the contractor is selected.

d. Provide the schedule of expected milestones in this project.

Response:

The time frames in which milestones will be completed is a matter that will be addressed through the contract bid process, so the schedule will not be determined until the contract is awarded (in fact, the schedule will not be finalized until the completion of a review scheduled to occur 6 weeks into the first phase). While the schedule will continue to be notional at the time of contract award, we would be pleased to provide it to the Committee at that time.

The attached chart (Enclosure B) depicts four notional phases, including project reviews, control gates, and other controls associated with each phase.

Phase I establishes a single point of entry for legacy case management; expands the search capability to include IntelPlus file rooms; provides browser access to investigative data without requiring that browsers understand the changes in system architecture; and subsumes and expands current Web-based Automated

Case Support (ACS) capabilities by summarizing a user's workload on a dashboard, rather than requiring the user to perform a series of queries to obtain it. To simplify data entry into the Universal Index (UNI), an entity extraction tool will be used to automatically index appropriate persons, places, and things. Finally, the core infrastructure components will be selected during this phase, and may include an Enterprise Service Bus and foundation services.

Phase II provides case document management and a records management repository, beginning the transition to paperless case records and implementing electronic records management. A workflow tool will support the flow of electronic case documents through their review and approval cycles, and a new security framework will support role-based access controls, single sign on, externally controlled interfaces, and electronic signatures based on Public Key Infrastructure. This phase addresses the concerns of the users of Sentinel's Initial Operating Capability that a paperless environment is necessary to leverage the benefits of automated workflow.

Phase III replaces and improves the Bureau-wide global index for persons, places, and things. In the "Connect the Dots" paradigm, the "dots" are represented by UNI, the legacy index that is, in effect, a database of entities (i.e., persons, places, and things) that have case relevance. Unlike the current UNI index, which supports a limited number of attributes, the new global index will improve the richness of the attributes associated with the indexed entities, permitting more precise searching.

Phase IV implements the new case and task management and reporting capabilities and will begin the systematic consolidation of case management systems.

e. Provide the system by which each stage of production of the program will be measured.

Response:

As indicated in response to Question 11d, above, the Sentinel program is employing a multi-tiered system of program management tools and practices to measure each stage of system development. Following are the three major program management tools and practices to be used by the Sentinel program.

1. Adherence to and expansion of the oversight process outlined in the FBI's IT LCMD. During each of the four phases of the Sentinel system's development, independent, senior executive boards will conduct six

separate control gate reviews. Each of these reviews must be favorable before Sentinel development can proceed. Each phase of the Sentinel system's development will also be the subject of 12 program-level reviews to measure that phase's progress. The standard FBI IT LCMD oversight and management process has been expanded for Sentinel by additionally requiring:

• An Acquisition Plan Review by the FBI Investment Management/Project Review Board before awarding contract options for Phases II, III, and IV.

• An Integrated Baseline Review immediately following the award of the base contract and each contract option to ensure EVMS policies and procedures are in place and adequate.

• A Delivery Acceptance Review near the end of each phase of Sentinel development to ensure that all work has been completed properly, including the training of field personnel and the accomplishment of organizational change management tasks.

2. Adherence to the use of EVMS principles and practices recommended by the Program Management Institute and Defense Acquisition University and mandated by the Office of Management and Budget. The Sentinel Program has embraced and mandated the use of EVMS principles and practices to measure the progress of each phase against an EVMS baseline (cost, schedule, and performance). The Sentinel Statement of Work requires that the provisions of FAR Case 2004-019 (published in the *Federal Register* on 4/8/05) be followed. Among other things, this requires the prime contractor to furnish a monthly progress report with respect to each phase's EVMS baseline and must provide the reasons for variances of more than five percent.

3. Use of an Independent Validation and Verification (IV&V) authority. Each phase of the Sentinel system's development will be independently measured and reported on by an IV&V authority. Throughout the development and deployment contract, this independent authority will measure progress and performance against the performance baseline. The results of these independent measurements will be reported to the FBI's CIO and PME.

12. The 9/11 Commission Staff Report no. 9 (pg. 9) faulted the FBI for having poorly trained and unqualified analysts.

a. Has the FBI changed its policy of hiring internally? Has there been any policy change that would allow for and that has resulted in the hiring of educated, trained and experienced analysts from external sources?

Response:

The 9/11 Commission's criticism of the qualifications of FBI analysts was based on an internal FBI document published in 1998 that asserted that two-thirds of FBI analysts were not qualified. The basis for the judgment expressed in that document is unclear and, in any event, is no longer accurate. In the 7 years since its publication, the FBI has established policies and systems to ensure the FBI's IAs are of the highest competence and quality. With the benefit of these new policies and systems, over the past two years we have hired more than 1,100 IA applicants possessing one or more critical skills. Of these recent hires, 59% had related intelligence or analytical experience, 47% had military experience, and 38% had advanced degrees.

A key component of this recent policy has been creation of the Intelligence Career Service (ICS), which demonstrates the importance of the FBI's intelligence mission and elevates the stature of its intelligence professionals. To develop the ICS, the FBI looked to both other elements of the USIC and the FBI's selection systems for best practices, creating a selection system implementation plan that would ensure selections based upon competencies identified for IAs, Language Analysts (LAs), and Physical Surveillance Specialists. (A "competency" is a cluster of related knowledge, skills, and abilities needed to perform a specific job.) These competencies correlate with job performance, can be measured against standards, and can be improved through training and development. Competency models allow for maximum reuse of human resources tools (such as testing and training courses) to assess and develop commonly required skills. Competency models also allow for the development of unique tools to assess and develop specialized skills. The competencies define our selection and hiring, training and development, performance management, Intelligence Officer Certification, retention, and career progression. They also help target and assess applicants, including those from within the FBI, with critical skills in intelligence, foreign languages, technology, area studies, and other specialties.

In furtherance of the effort to attract and retain IAs with critical skills, the FBI has also implemented three scholarship programs:

1. The Pat Roberts Intelligence Scholarship Program (PRISP) enhances the FBI's retention of IAs with specialized critical skills. Through the PRISP, the FBI can grant $25,000 scholarships to current employees to help fund their past, current, or future studies in specialized skills or areas deemed critical by the FBI.

2. The Cooperative Education Program offers to college juniors and seniors who are pursuing studies in critical Intelligence Program skills the opportunity to attend school full-time during part of the year and work at the FBI full-time during part of the year. Program participants receive FBI salaries and benefits, as well as tuition assistance.

3. The Educational Attainment Internship provides financial assistance to selected high school seniors who will be pursuing college level work in a discipline deemed operationally critical to the FBI.

b. How many analysts have been hired since 9/11 from external sources?

c. How many analysts have been hired since 9/11 from internal sources?

Response to subparts b and c:

As indicated below, FBI records indicate that from FY 2002 through 8/18/05 the FBI has hired 377 IAs from within the FBI and 958 from outside the FBI (the number of external hires may include some FBI personnel who applied to external job postings). Regardless of the source of the candidate, all IA candidates are selected according to the same competency-based criteria, and successful IA candidates must meet these criteria.

Fiscal Year	Internal Sources	External Sources
2002	56	40
2003	77	173
2004	141	208
2005 (thru 8/18/05)	103	537

13. Since 9/11, the FBI continued to be plagued by a shortage of qualified analysts and translators. In the *New Yorker* article, the New York Police Department (NYPD) was able to resolve their analyst and translator problem by drawing upon immigrants who were intimately familiar with the languages and cultures under survey (pg. 64). These languages included Farsi, Arabic, Pashto, Dari and 60 other languages.

a. Has the FBI launched a similar program to address this issue?

b. If not, why not?

Response to subparts a and b:

For the last several years, the FBI has aggressively recruited from ethnically diverse communities throughout the United States to meet its translation requirements. In addition to traditional media campaigns, the FBI's National Recruiting Team and DI personnel have targeted specialty conferences, career fairs, university foreign language departments, and other forums to recruit those with critical language skills. FBI management officials also regularly host community meetings and speak at local events to generate interest in FBI employment and contractor opportunities. Beyond this, the FBI has partnered with organizations such as the U.S. Copts Association, Arab American Anti-Discrimination Committee, Arab American Institute, Network of Arab American Professionals, and Muslim Public Affairs Council to establish good will with their membership and to encourage those with critical language skills to consider FBI employment. Collectively, these efforts have resulted in more than 80,000 applications for linguist positions since 9/11/01 (most often, FBI linguists begin as contract linguists, so the majority of these applications have been for contract linguist positions that often evolve into FBI employment as LAs).

More than 3,000 FBI employees and contractors, including 397 LAs and 1,004 contract linguists, now have certified foreign language proficiency scores at or above the working proficiency level. More than 95% of the FBI's linguists are native speakers of a foreign language. These native-level fluencies and long-term immersions in foreign cultures ensure firm grasps of not only colloquial and idiomatic speech but also of heavily nuanced language containing religious, cultural, and historical references. Trustworthiness, as demonstrated through the security clearance process, is, of course, required of all FBI employees, including linguists.

14. This same article reports that the CIA and Pentagon have both asked the NYPD to assist them with translations, investigations and analysis of information relating to national security (pg. 64).

a. Has the FBI made use of the NYPD translation and analysis program?

b. If not, why not?

c. If so, set forth those instances in which the NYPD program has been used by FBI?

Response to subparts a, b, and c:

The FBI has not made use of the NYPD's translation and analysis program. In 2003, the FBI's Chief of Language Services met with the Deputy Commissioner of the NYPD to discuss common translation challenges and to explore the feasibility of sharing translation resources. During this meeting, the NYPD indicated that it did not want its officers and translation staff to undergo FBI polygraph examinations as a condition of their access to FBI information (the FBI requires that all candidates for its translator position submit to polygraph testing as a condition of being granted access to national security information). We understand that the CIA and Pentagon have found a means of ensuring trustworthiness without the use of polygraph examinations. We will work with both organizations to learn more about this process and will evaluate our ability to do the same.

15. The NYPD recruits immigrants from the Asia, Africa and the Pacific Islands to find qualified analysts and translators.

a. Does the FBI have a similar recruiting policy in place that targets immigrants?

b. If not, why not?

c. If so, provide statistics showing the results of this recruitment effort.

Response to subparts a, b, and c:

The FBI makes extensive use of LAs recruited from immigrant communities. We hire from those communities consistent with Executive Order (EO) 12968, "Access to Classified Information," which provides that "access to classified information shall be granted only to employees who are United States citizens".

(Section 3.1(b)). This EO substantially limits the FBI's ability to use the services of non-citizens, because nearly all of the FBI's CT and CI information in need of translation is classified at the "Secret" or "Top Secret" level. The EO does not, however, apply to state and local law enforcement agencies, who are free to establish their own standards for access to law enforcement information and may therefore obtain the assistance of immigrants without U.S. citizenship to meet translation requirements.

16. On multiple occasions the FBI has been criticized for having thousands of hours of untranslated terror intercepts, including most recently in the OIG report dated July 27, 2005. One of the FBI's reasons for the backlog of untranslated intercepts is the lack of cleared analysts and translators.

a. Would the FBI agree to certify local or state law enforcement security checks for the purpose of clearing analysts and translators to assist the FBI?

b. If not, why not?

Response to subparts a and b:

The FBI can authorize state or local law enforcement to conduct security checks of analysts and translators if those authorities conduct the checks in accordance with EO 12968. Generally, the requirements of EO 12968 are not met by state and local law enforcement agencies.

c. Is it true as the OIG reports that it takes the FBI an average of 16 months to hire a contract linguist - an increase in time from prior years studied?

Response:

An audit conducted by the DOJ Office of Inspector General (OIG) during 2003-2004 used the averages of the four applicant processing stages to determine a total cycle time of 14 months. A subsequent OIG audit adopted an entirely different methodology, including periods of time beyond the FBI's control, to determine that the total cycle time is, instead, 16 months. The difference between the 14-month and 16-month processing times is accounted for by these periods beyond the FBI's control, such as periods in which an applicant is out of the country and therefore unavailable for polygraph.

The FBI believes that the better measure of our processing efficiency is the 14-month applicant processing time. Under this methodology, a contract linguist candidate who successfully completes each stage of the employment process can

expect to remain in the process for 425 days before receiving the required "Top Secret" security clearance.

Contract Linguist Applicant Cycle (FYs 2004-2005)				
Phase	**Annual Volume**	**Pass Rate**	**Current Cycle Times (Median)**	**FY 07 Target (Approximate)**
Professional Testing	3,000	25%	158 days	60 days
Polygraph	600	58%	65 days	30 days
Background Investigation	350	85%	95 days	60 days
Security Adjudication	300	90%	107 days	30 days
Total	**270**	**13%**	**425 days**	**180 days**

All contract linguist candidates are subject to a thorough pre-contract vetting process that is both labor and time intensive. Contract linguist candidates must pass proficiency tests in both English and a foreign language. In addition, because they must be granted "Top Secret" security clearances, each candidate's pre-contract vetting process includes the following:

- Personnel security interview conducted by appropriately trained FBI SA or security personnel.
- Polygraph examination focused on the candidate's involvement in foreign counterintelligence matters, purpose in seeking FBI employment, application accuracy and thoroughness, and prior involvement in the sale or use of illegal drugs.
- Single-scope background investigation covering the most recent 10-year period of the candidate's life or longer.
- Risk analysis of the background investigation package conducted by FBI CI and/or CT subject matter experts.

d. If true, how can FBI hire qualified, highly marketable, people when they must wait over a year to find out if they are going to be hired?

Response:

The FBI shares your concern. We are working to reduce the time required for the applicant vetting process from 425 days to approximately 180 days by FY 2007 through the implementation of process improvements recommended by a business process reengineering firm and the National Academy of Public Administration. Among other means to this goal, the FBI plans reduce the proficiency test cycle from 158 to 60 days by the end of FY 2006 by automating its language proficiency test instruments and using third party test centers. The FBI also anticipates reducing the background investigation and security adjudication cycles from approximately 200 days to 90 days by FY 2007 by consolidating background investigation functions within the Security Division and reorganizing to streamline associated activities.

e. If true, do the inevitable changes in the terrorist landscape and therefore the particular languages in need of translation, require an expedited hiring process in order to keep up with the ever changing war on terrorism?

Response:

The FBI can and often does respond to operational exigencies through the expedited processing of contract linguist candidates. For example, in 2005 several contract linguist candidates with proficiency in an urgently needed African language were recruited and fully vetted through proficiency testing, polygraph, and background investigation in 30 days or less. This rapid response capability, while extremely manpower intensive, ensures the FBI can quickly respond to the most critical national security requirements.

The FBI recognizes that with the ever-changing face and voice of global terrorism, we must be prepared to respond to translation requirements associated with the world's most obscure languages. Geopolitical indicators and threat forecasts provide a foundation for the FBI's translation planning.

f. If untrue, how long does it take FBI, on average to hire contract linguists and is this time reasonable?

Response:

Please see our response to Question 16c, above.

17. The FBI translation program has been criticized for having excessive and unreasonably high standards when it comes to pre employment language testing. There have been newspaper articles detailing that, for instance, University Professors who teach Arabic were unable to pass the test.

a. Is the FBI testing standard [ ] too high?

b. What, if any, changes are planned in this testing process to avoid these unreasonably high testing standards?

Response to subparts a and b:

The FBI evaluates language tests in accordance with Interagency Language Roundtable (ILR) Skill Level Descriptions, approved by the Office of Personnel Management as the standards for government-wide use in 1985, and uses the Defense Language Proficiency Test, prepared by the Defense Language Institute, to test foreign language listening and reading skills. The ILR employs a scale of 0 to 5, describing Level 2 as "Limited Working Proficiency" and Level 3 as "General Professional Proficiency."

The passing score for FBI verbatim translation exams is 2+ or 3, depending on the score received in the speaking proficiency test. When applicants with knowledge of a foreign language fail a translation test it is typically because good translation requires not only proficiency in two languages but also what the ILR describes as "congruity judgment," or the ability to choose the best accurate equivalent from among possible translations.

18. With the recent terrorist attacks in London, intelligence analysts are saying, and the American public is concerned, that an attack on American soil is imminent.

a. How is the intelligence community – FBI, ISE, DOJ – preparing to protect us against such an attack?

Response:

In response to the London mass transit attacks, the FBI has been assisting British authorities in their investigation and has been investigating any and all connections to the U.S. to prevent a similar attack here. One phase of this effort has been the production of an unclassified daily Intelligence Bulletin that communicates current investigative updates and other information that might be useful to state and local law enforcement authorities. Among other things, these bulletins have articulated the tactics and techniques used in the London bombings and detailed the chemical composition of the explosives used in the attacks. These bulletins have been provided to all FBI field offices and to our law enforcement partners.

b. What has the FBI learned from the London attacks that can help prevent a mass transit attack in the U.S.?

Response:

The FBI continues to investigate the London bombers' relationships and contacts, including their financial and communications links, to identify any persons who might pose a danger to the U.S. We remain concerned that the London attacks could serve as a template for an attack in the U.S. in which a few "home grown" extremists might target a metropolitan subway system using relatively small quantities of homemade explosives. The FBI is more committed than ever to working collaboratively with state and local law enforcement, who are often the most effective first line of defense in identifying and disrupting attacks.

19. In testimony before the Senate Committee on Foreign Relations in 2002, President Henry Kelly of the Federation of American Scientists reported that "significant quantities of radioactive material have been lost or stolen from US facilities in the past few years." He also stated that much of this material is useful for the construction of radiological dispersion devices and dirty bombs.

a. What is the FBI doing to track and recover lost or stolen radiological material in the U.S.?

Response:

The FBI maintains a close relationship with the agencies involved in licensing the possession of nuclear/radiological material (including the Department of Defense (DoD), Department of Energy (DoE), and Nuclear Regulatory Commission (NRC)). Pursuant to the FBI's Nuclear Site Security Program, we have directed our field offices to establish close liaison with appropriate security personnel at nuclear sites in order to ensure prompt notification and response to suspicious activity, including attempts to illegally obtain nuclear or radiological material. We have also reiterated to all field offices the need for aggressive investigation of lost, stolen, or missing radioactive source material and the importance of ensuring that state and local law enforcement authorities promptly notify the FBI of such incidents. Coordination of these issues has been greatly facilitated by the development and enhancement of the JTTF program because the JTTFs, which are comprised of federal, state, and local law enforcement representatives, are invaluable assets in the sharing of information and coordination among law enforcement agencies. The FBI also participates in a number of interagency working groups at the Headquarters level in order to develop U.S. Government policy options for preparing for, preventing, responding to, and recovering from a radiological attack. These working groups have undertaken numerous tasks, including the review of existing security and licensing regulations for adequacy and appropriateness and the development of a National Source Tracking System to better account for individual radiological sources in the possession of NRC licensees, which include medical, industrial, and academic entities.

b. Provide a list of all known lost or stolen radiological material in the U.S.

Response:

The NRC-managed Nuclear Materials Event Database indicates that since January 2003 NRC licensees reported approximately 1,300 events involving lost, stolen, or abandoned radiological sources. The NRC estimates that approximately 50 percent of these radiological sources are eventually recovered.

While statistics such as these may appear to indicate a significant loss of material, the majority of these incidents involve minute quantities of radioactive material present in industrial equipment used in radiography and well logging. Such equipment often contains "low hazard" material with a short half-life. While the FBI is concerned with all reports of lost, missing, or stolen nuclear or radiological material, and coordinates closely with the cognizant agencies in aggressively investigating these allegations, the vast majority of these incidents appear to be inadvertent rather than the product of criminal intent, do not pose a harm to public safety, and are therefore not considered "significant" for CT purposes.

20. There are currently seven sites in the U.S. that handle Category I special nuclear material, or nuclear material that is considered weapons-grade material.

a. What role does the FBI have in securing this material from theft?

Response:

The FBI is responsible for investigating allegations of unlawful use or possession of nuclear or radiological materials, and threats to use such materials, for terrorist or other criminal purposes. This responsibility includes all man-made radiological materials (those used in reactor operations as opposed to those that occur naturally), which may run the gamut from weapons-grade materials (Category I Special Nuclear Material (SNM)) to radiological source materials. Such misuse may be prosecuted through a variety of statutes.

DoE's National Nuclear Security Administration (DoE/NNSA) bears primary responsibility for the safety and security of its nuclear facilities, including those that handle Category I SNM. As part of its overall Nuclear Site Security Program, the FBI coordinates closely with these sites in a proactive effort to prevent terrorist or other criminal activities directed against these sites. Such efforts include both routine liaison activities (such as intelligence sharing and threat briefings) and more specialized initiatives (such as joint training and exercises that typically focus on the coordination of emergency responses to potentially disruptive incidents).

b. Is there a policy of standardized security procedures that must be followed by such facilities?

Response:

DoE/NNSA adheres to an extremely rigorous and robust protection strategy based on the sensitive nature of the assets under its purview. This protection strategy is "graded" according to the type of material handled at a given site, with Category I SNM sites afforded the highest level of protection. Further information on this subject may best be obtained from DoE.

c. If so, provide the standard security procedures and how these procedures are monitored by FBI.

d. If not, are there any written plans to do so? Provide written plans.

Response to subparts c and d:

Security countermeasures are part of each site's protection strategy. The FBI is not responsible for monitoring DoE's protection strategy per se, but we do maintain a level of interaction with DoE through regularly recurring liaison and training, and this interaction facilitates a regular review of these procedures.

21. In recent years, there have been a number of reported incidences of theft of documents and materials from Los Alamos National Nuclear Laboratory and other locations.

a. How does the FBI plan to reduce the number of thefts from these facilities?

Response:

Pursuant to 50 U.S.C. § 402a, the FBI is to be "advised immediately of any information, regardless of origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power." The FBI has initiated proactive measures in order to better protect against the compromise of classified information, specifically addressing compromises in the national laboratories. The cornerstone of these measures is the Agents in the Lab Initiative.

Pursuant to this initiative, FBI SAs are embedded in the Internal Security Office of the Los Alamos National Laboratory (LANL). These SAs possess academic

credentials in mechanical and nuclear engineering, which lend themselves to the LANL's overall scientific and research mission. The LANL's Internal Security Office is responsible for the Lab's counterintelligence (CI) and counterterrorism (CT) activities, including: the conduct of CI briefings/debriefings for LANL personnel; response to internal CI inquiries regarding LANL employees, contractors, and visitors; and the identification of potential CI and CT risks and exposures to Foreign Intelligence Services and terrorist organizations. The FBI has also assigned an experienced Sante Fe Supervisory Senior Resident Agent (SSRA) to focus on day-to-day LANL operations, permitting emphasis on espionage prevention and detection and strong partnerships with DoE and the CIA.

When FBI SAs investigate matters at the LANL, they share the resulting reports with DoE entities, including the LANL. DoE/NNSA uses these reports to develop "lessons learned" reports, identifying potential weaknesses in the internal security apparatus and providing recommendations to resolve concerns. In addition, the FBI's Albuquerque Division SAC meets regularly with the LANL Director to discuss all matters of interest. That meeting is attended by the Santa Fe SSRA and the LANL's Senior CI Official (who heads the Internal Security Office); the Santa Fe SSRA and LANL's Senior CI Official also meet separately each month to ensure maximum information sharing.

Additional information responsive to this inquiry is classified and is, therefore, provided separately.

b. Has FBI investigated these incidences?

Response:

The FBI thoroughly investigates all reports of possible theft or compromise of classified documents or materials. Previous cases have been successfully resolved and future incidents are much less likely due to the implementation of more effective and efficient administrative and security practices.

c. How many such incidences remain unsolved? Provide date, time, location and circumstances regarding such unsolved incidences.

Response:

The response to this inquiry is classified and is, therefore, provided separately.

22. The NYPD currently treats all tractor-trailer and hazmat incidences as potential crime scenes, due to intelligence received about al Qaeda operating procedures.

a. Does the FBI have clearly defined procedures in place to facilitate cooperation between the FBI and local and state law enforcement officials to determine if an incident is an accident or a terrorist attack?

Response:

The FBI's responses to all threats and incidents involving potential weapons of mass destruction (WMD) or other terrorist acts include assessments of credibility and interagency coordination. Typically, FBIHQ is notified of a suspected WMD threat or incident by the FBI field office in the location of the threat or incident. Upon such notification, or when FBIHQ otherwise becomes aware of such threats or incidents, FBIHQ's WMD Operations Unit (WMDOU) provides rapid assistance to the field, including execution of the following standard operating procedures:

1. Evaluation of the initial threat assessment (that initial threat assessment is often conducted by the FBI field office).
2. Completion of a comprehensive threat assessment.
3. Coordination of FBIHQ assets for response and the provision of technical support.

WMDOU, which is responsible for developing appropriate FBI response policy for such incidents, overseeing strategic threat assessments, and coordinating assets to assist FBI field divisions in their responses to domestic WMD threats or incidents, uses the threat assessment process to identify the resources needed for response. WMDOU calls on previously identified subject matter experts in other agencies and consults with FBI scientists and the FBI's Hazardous Materials Response Unit as appropriate to the incident. These technical experts are able to respond to chemical, biological, and radiological/nuclear incidents, as well as incidents involving explosive devices. In addition, FBI field offices have designated WMD Coordinators, who are responsible for developing strong relationships with federal, state, and local crisis and consequence management agencies. WMD Coordinators also maintain liaison with a wide range of emergency responders through the JTTFs (each of which includes representatives from state and local government) and participate in operational crisis response training and exercises with state and local counterparts. During a potential terrorist incident, the FBI would notify JTTF members so the response may be coordinated appropriately with law enforcement partners at all levels.

b. If so, provide a copy of those procedures and a description of all incidences in which the procedures have been implemented.

Response:

Both FBIHQ's WMDOU and FBI field offices respond to large volumes of threats, rendering it impracticable to provide an exhaustive list describing these incidents.

Homeland Security Presidential Directive 5 required the development of a National Response Plan (NRP) to align Federal coordination structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic incident management. The 426-page NRP, which is available in full on DHS's website, provides the protocols for response to domestic incidents, including nuclear and radiological incidents, biological incidents, and other acts of terrorism. While much of the NRP concerns response to incidents such as the tractor/trailer and hazardous materials incidents on which this question focuses, the most relevant portions of the NRP are the Terrorism Incident Law Enforcement and Investigation Annex, the Nuclear/Radiological Incident Annex, and the Biological Incident Annex. Those three annexes are attached (Enclosure C).

Questions Posed by Senator Leahy

23. In follow up questions to a June 6, 2002, hearing, you stated that agents at headquarters should have expertise in areas to which they are assigned. This would certainly include counterterrorism officials. You also said that field supervisors should have "extensive counterterrorism experience." Recently, we learned from depositions in a civil suit that the highest level of counterterrorism officials at the Bureau do not have specific prior experience in this area, nor do they think it is important for them to possess such expertise.

a. How can we reform the FBI if it insists that traditional law enforcement experience is *all* that is needed to prevent and prosecute acts of terrorism?

Response:

We respectfully disagree with the assertion the FBI "insists that traditional law enforcement experience is *all* that is needed" to prevent terrorism. SA candidates for positions in all programs are required to demonstrate levels of experience and performance appropriate to the position, and increasingly rigorous standards are applied to progressively higher leadership levels.

Candidates for all SA mid-level management positions (generally, those at the GS-14 and GS-15 levels) are vetted through selection boards comprised of Senior Executive Service (SES) members representing priority divisions at FBIHQ, including CTD, CD, DI, CyD, and CID. For example, ASAC candidates (ASAC is a GS-15 position) are required to demonstrate competence in the following areas through the submission of two examples with respect to each area: communication, flexibility/adaptability, initiative, interpersonal ability, leadership, liaison, organizing and planning, and problem solving/judgment. Often, these examples identify the impact of the candidate's efforts on the FBI's highest priority matters, including CT accomplishments. Mid-level SA managers seeking promotion to entry level SES positions are required to submit résumés demonstrating success in five competencies: management, leadership, liaison, problem solving, and interpersonal ability. Within these competencies, candidates must show the highest levels of achievement in the FBI's top priorities. To the extent possible, these résumés also reflect successes in program areas applicable to the position being sought.

Throughout these multi-tiered vetting processes, strong managerial skills are considered critical, and subject matter expertise is considered and preferred, but is not mandatory. Typically, SAs who attain higher-level executive positions have first held other senior management positions in the FBI, such as SAC of a field

office, and through them have acquired management experience across both national security and criminal programs.

b. Do you think that law enforcement experience is sufficient? Or do you believe that expertise in counterterrorism should be a prerequisite for counterterrorism leaders of the Bureau?

Response:

After the events of 09/11/01, the FBI's top priority became the prevention of additional terrorist attacks against this nation. As part of this mission shift, we initiated the development of career paths for SAs that will require them to specialize in one of five areas: CT, CI, intelligence, cyber, or criminal. As this policy is implemented, the FBI will develop a cadre of SAs with subject matter expertise in each of these priority programs. Once this cadre is established, it may be appropriate for the FBI to consider mandatory subject matter expertise in certain positions. In the meantime, we believe it is appropriate to consider subject matter expertise as a factor, but not a prerequisite, when determining assignments.

Among the FBI's efforts to foster growth in these priority areas is a rotational program pursuant to which SAs are assigned to FBIHQ on a temporary duty (TDY) basis to address priority program needs. This program allows "field" Agents to bring "real world" experience to FBIHQ and to learn more about the "big picture" than is possible when working isolated cases. In FY 2004 alone, approximately 2,200 SAs benefitted from these TDY assignments.

24. A panelist participating in the 9/11 Commission's Public Discourse Project reported that the Bureau has 200 unfilled counterterrorism positions and is facing difficulty finding analysts and agents to fill those posts.

a. How many counterterrorism positions at the Bureau are presently unfilled? What are the obstacles to filling these positions?

Response:

As of 05/13/2005, there were approximately 202 vacant SA CT positions at FBIHQ. The primary obstacles to filling these positions, and positions at FBIHQ in general, are the recent spike in D.C.-area housing costs and the overall high cost of living in the Washington, D.C., area.

The FBI's success in recruiting analysts has been better. The FBI's FY 2005 goal was to hire 880 analysts. As of 8/29/05, we had hired 660 new analysts (including both external hires and applications from qualified FBI employees serving in other positions). An additional 376 applicants have been selected and are being processed for employment, and 72 analyst candidates have been approved for employment but are not yet on board. During the same time period, 103 analysts have vacated analyst positions through reassignment, transfer to other federal agencies, resignation, or retirement. These numbers indicate that there are no particular obstacles to filling analyst positions, but there is some difficulty in keeping analysts on board.

b. What steps has the Bureau taken to fill these positions more rapidly?

Response:

To ensure a constant flow of applicants for all critical positions, the FBI attempts to publicize the rewards of FBI careers through various means, such as national advertising strategies targeting applicants with critical skills, including minorities, women, and persons with disabilities. These strategies include interactive campaigns and targeted advertisements in magazines, journals, television, radio, billboards, airports, newspapers, and theaters. The advertisements feature onboard employees who have critical experience and education that matches the FBI's targeted hiring objectives. This year's special effort to attract applicants to the analyst positions included a television ad that aired during the 2005 Super Bowl.

In addition, partnerships and networking vehicles have been developed to expand awareness of the FBI's career opportunities within the African-American, Asian-American, Hispanic, Native American, and Middle Eastern communities, and by addressing women's organizations and physically challenged audiences. The FBI has also developed partnerships with faith-based organizations to improve awareness of the FBI in those communities, and has implemented numerous internship programs in order to enhance the FBI's visibility and recruitment efforts at colleges and universities throughout the United States.

In addition to attracting and retaining critical employees through the increased use of the student loan repayment program and relocation and retention bonuses, the FBI has developed an FBIHQ Term Temporary Duty Pilot Program, pursuant to which SAs may apply for designated 18-month term FBIHQ assignments during a 90-day window. Selectees will receive FBIHQ supervisory credit and will be authorized to apply for field desks as SSAs after 15 months. As of 08/30/2005,

this pilot project had generated 567 applications for positions at FBIHQ and is expected to greatly reduce the staffing shortfall.

Similarly, a combination of methods is being employed to fill analyst positions quickly and to keep them filled. Recruitment bonuses totaling approximately $3.4 million were paid to approximately 380 analysts and retention allowances were afforded to two analysts in approximately the first 10 months of FY 2005 (many analysts are fairly new to the FBI and are not yet eligible for retention incentives). The availability of these bonuses is beneficial both because they encourage applicants to apply for analyst positions and because they encourage them to stay to complete the service to which they agree as part of the bonus offer. Retention has also been improved by our ability to increase access to the student loan repayment program, which also includes a service commitment. Whereas the availability of funds limited participation to 31 analysts during FY 2005, approximately 180 analysts participated in the student loan repayment program during FY 2005.

25. In July, John Perry, chief executive of CardSystems, testified before the House Financial Services Subcommittee on oversight and Investigations about a security breach that exposed as many as 40 million credit-card holders to potential fraud. Mr. Perry testified that CardSystems contacted the FBI about the data breach on May 23, but that the FBI took two days to respond, in part due to lack of clarity on the scope of the breach.

What is the FBI's policy on responding to reports of personal data security breaches, including how quickly agents should respond to such reports, and what expertise and forensic capabilities are available within the FBI to assess the scope of electronic data breaches?

Response:

With respect to the CardSystems Solutions, Inc. (CSSI) breach, we would like to note that the FBI initiated investigation on the day it was contacted based on information provided by the CSSI General Counsel to the FBI's Phoenix Division. At that point, CSSI had already determined that the intruder had been active within CSSI's network for nine months and CSSI had implemented defensive measures to mitigate further compromise. These measures included attempts to determine the type of data compromised and the extent of the breach, during which CSSI used the file transfer protocol to improperly retrieve from the intruder's computer the files that contained crucial transaction data and corresponding security codes obtained by the intruder through unauthorized queries. It was after this discovery that the FBI was notified, 8 days after CSSI noticed the unauthorized activity and 4 months after CSSI was alerted by the card

associations that they believed other unusual activity could be traced to a possible compromise of CSSI data.

As with all information of possible criminal activity received by the FBI, information relating to possible computer intrusions is initially evaluated to determine the appropriate course of action. The FBI's response depends on the circumstances involved: is there a possibility of loss of life, terrorist attack, state-sponsored intrusion placing the national information infrastructure at risk, prevention of criminal activity or further financial loss? (In the CSSI case, the FBI was advised that CSSI had implemented defensive measures to mitigate further compromise.)

The FBI's CyD includes the Special Technologies and Applications Section (STAS), which is often called upon by other FBI Divisions, USIC agencies, state and local governments, and foreign partners to determine the "who, what, why, when, where, and how" of computer intrusions. Through written reports, electronic disseminations, and other means, the STAS helps IAs, investigators, and decision makers understand what level of sophistication the activity represents, where evidence of the intrusion may be located, and, in some cases most importantly, what data was viewed, modified, added, deleted, or taken, and where it might reside thereafter. STAS is commonly called upon to re-live the electronic "day in the life of a computer file" to explain who saw it, "touched" it, moved it, and so on.

26. A June 2005 report by the Office of Inspector General evaluated DOJ's counter-terrorism task forces and advisory counsels, including 3 led by the FBI: the Joint Terrorism Task Forces (JTTFs), the National Joint Terrorism Task Force (NJTTF) and the Foreign Terrorist Tracking Task Force (FTTF).

a. The report found management and resources problems, including frequent turnover in leadership of the JTTFs, lack of counterterrorism expertise within the task force membership, as well as insufficient training, standards or orientation for members. What specific actions will the FBI undertake to address these concerns?

Response:

The FBI concurs with the findings of the DOJ Office of the Inspector General (OIG) regarding the importance of ensuring long-term, stable JTTF and Foreign Terrorist Tracking Task Force (FTTTF) leadership, effective and available training in critical substantive areas, and, in the case of the FTTTF, a settled location.

All FBI investigators, in all programs, view the quality and completion of investigations as a priority. JTTF participants currently receive training in basic core functions, and training has been developed and delivered (in various formats) regarding the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, basic security issues (including the proper classification of intelligence communications), the roles, missions, and operations of the USIC, the FBI's ACS system, the Investigative Data Warehouse (IDW), the Threat Reporting System, and the tools, techniques, and skills needed to successfully investigate terrorism.

A recently created CTD Unit has been charged with assessing CT training and professional development needs, including those of the JTTFs. This Unit is developing a comprehensive NJTTF/JTTF Training Manual that will include the topics listed below. These topics will also be addressed in training provided to newly appointed JTTF members within their first year of service.

- Administration
- Security
- Automation/Computer Investigative Resources
- Introduction to Foreign Intelligence/Terrorism
- International/Domestic Terrorism Basic Courses (CD-ROM based training)
- Foreign CI Basic Course (CD-ROM based training)
- Surveillance Techniques
- Evidence Procedures
- Technical Writing
- Legal Training
- Asset/Source Recruitment and Management

The FTTTF has faced numerous challenges since its creation, and the pursuit of some of its own initiatives have been delayed while it provided critical support to the early efforts of the TSC, which was also recently created. The FTTTF has addressed the early problems created by fluid leadership and organizational structure, and has recently been relocated to "permanent" space, which will further improve stability. The FBI concurs with the OIG's recommendation that the FTTTF develop and implement a marketing plan to improve awareness and understanding of its services, and has taken steps to implement such a plan. The FTTTF's efforts to increase awareness of its role and responsibilities have included weekly briefings to visiting SACs and ASACs, participation in CTD's orientation program for new assignees, presentations to the NJTTF Conference, briefings to new SACs and Legal Attachés, and briefings to outside organizations (including the International Association of Chief of Police, National Sheriffs'

Association, Major City Chiefs, Interagency Intelligence Committee on Terrorism, and Homeland Security and Information Sharing Conference). In addition, the FTTTF has established a site on the FBI's Intranet, which will be replicated in part on the Secret Internet Protocol Router Network, and has published an Executive Guide to provide a concise synopsis of FTTTF capabilities and the means of requesting support.

b. In addition, the OIG report noted that the FBI has not signed Memorandums of Understanding (MOU) to define the roles, responsibilities, information sharing protocols and length of commitment with the agencies participating in these taskforces. When will the FBI have in place an MOU defining these critical elements?

Response:

Since 1980, the FBI has maintained Memoranda of Understanding (MOUs) with the state and local agencies that participate in the JTTFs. The FBI currently has in place 311 MOUs with agencies participating in the NJTTF and JTTFs, updated since 9/11/01 to incorporate such issues as polygraph requirements, information sharing policy, and length of commitment by individual participants. The FBI's CTD is currently working with DoD and DHS to standardize these MOUs and anticipates that the existing MOUs will be updated in the near future.

27. A recent report by the National Academy of Public Administration found that the FBI's information sharing practices are largely ad hoc with no mechanisms, such as penalties or incentives, to enforce or promote information sharing.

a. What progress has the FBI made in creating incentives to improve information sharing and penalties for failure to advance those goals?

b. What future actions does the FBI plan to improve its information sharing capabilities further?

Response to subparts a and b:

Please see our response to Question 6, above.

28. In May of this year, it was reported that a search of IAFIS failed to identify the fingerprints of an individual detained by local authorities, Jeremy Jones, who was subsequently released and went on to kill three women and one teenage girl in three states. In addition, Mr. Jones is a person of interest in several other cases. An FBI official described the mistake as a "result of a technical database error, not a human examiner failing to make an appropriate match." What steps has the FBI taken to correct this database error and prevent a repeat of this type of mistake in the future?

Response:

The cause of the missed identification was a filter in the Automated Fingerprint Identification System (AFIS) component of the Integrated Automated Fingerprint Identification System (IAFIS). This filter, which was employed to narrow the field of records searched, erroneously eliminated Jones' record as a candidate because it was slightly outside the filter's parameters. When the FBI discovered this problem, it reviewed the need for the filter. Because of AFIS hardware upgrades completed in June 2004, it was determined that the filter was no longer necessary and should be disabled. This was accomplished on 1/9/05.

In addition to disabling the problematic filter, the FBI has taken several steps to ensure IAFIS' integrity. These steps have included an inspection of the system and the events that led to the missed identification, a search of the database to identify duplicate criminal history records, and the initiation of an aggressive program to detect and prevent missed IAFIS identifications. This program includes a quality assurance review of approximately ten percent of all transactions. In addition, because Jones used the exact name, date of birth, and social security number of another subject who was in prison at the time, causing additional confusion in making the identification, the FBI has initiated a review of all records that have exact matches of descriptive information to ensure they are not duplicate records and to provide investigative leads to law enforcement. Finally, the FBI has received funding for a 2006 effort to implement an overall enhancement of IAFIS that will involve substantial upgrades to the AFIS component. This broad enhancement was first conceptualized by the FBI, along with its law enforcement partners, in September 2003.

29. The consolidated watchlist uses 4 risk-based handling codes to designate how law enforcement should respond when encountering individuals on the list. A recent Inspector General report found that nearly 32,000 "armed and dangerous" individuals are designated for the lowest handling code. This code does not require law enforcement encountering those individuals to contact the TSC or any other law enforcement agency. Some of these individuals were also described as "having engaged in terrorism," "likely to engage in terrorism if they enter the Untied States," "hijacker," "hostage taker," and "user of explosive or firearms." In press reports, the FBI has countered that legal restrictions prevent officers from ordering a suspect held without an arrest warrant or other evidence.

Notwithstanding strategic reasons or legal requirements that weigh against immediate detention of these individuals, there is a legitimate concern about designating such individuals for the lowest handling. You indicated at the July 27 hearing that you would look into the matter and respond.

a. Why are individuals described in such dangerous terms designated for the lowest handling?

b. Is there a code that would allow TSC to designate these individuals in such a way that law enforcement encountering them would be aware of the possible danger or use the opportunity to update TSC on any encounters with those individuals?

Response to subparts a and b:

Director Mueller provided this information to Senator Leahy by letter dated 8/1/05. A copy of that letter is attached as Enclosure D.

It is important to understand that Handling Codes (HCs) are not associated with threat levels; all terrorism-related entries in the Violent Gang and Terrorist Offender File (VGTOF) are assigned HCs, and the first line on the NCIC screen for all these entries advises: "Warning, approach with caution." The purpose of assigning the different HCs is to identify the government's authority to take legal action with respect to the individual based solely on the individual's inclusion in VGTOF. Encounters with some of the 9/11/01 hijackers shortly before those attacks taught us the importance of arresting, detaining, or otherwise appropriately responding when those who pose a terrorist threat are encountered. If a local law enforcement officer encounters an individual for whom there is a pending arrest warrant related to terrorism (HC1), the officer needs to know to effect an immediate arrest. Similarly, a law enforcement officer who encounters an individual of investigative interest with respect to terrorist activity (HC2) needs to know to detain that person to obtain more information. Clearly, these individuals may be equally dangerous, so the HC doesn't identify the degree of danger they

pose to the law enforcement officer (in fact, the HC1 may be based on a warrant related to "white collar" terrorism financing, while the HC2 may be based on facts indicating bomb construction, so an HC2 could, in fact, be more dangerous to the officer than an HC1). Instead, the HC indicates what response by law enforcement is lawful and appropriate (arrest, detention, or otherwise) based on the information available to the TSC. All HCs request TSC notification so the TSC can assist in coordinating the response, and all HCs are subject to revision based on new information or changes in status.

HCs, which identify the permissible response if an individual is encountered, are unrelated to Immigration and Nationality Act (INA) codes, which are assigned by DHS to identify the nature of the derogatory information on an individual. We defer to DHS with respect to the assignment and use of INA codes.

30. The OIG Report found that there is "no formal strategic plan" to guide the [Terrorist Screening] Center's progress, staffing, structure and future planning, but that such a plan would assist the TSC in addressing the most significant weaknesses identified in the OIG report. In addition, the Report noted that TSC has no formal procedure for evaluating its own performance. When will the TSC develop a formal strategic plan or procedures for performance evaluation?

Response:

The TSC's formal strategic plan, dated 6/17/05, addresses the organization, structure, and progress of the TSC, including new initiatives, plan implementation, and progress reviews. The TSC's performance will be evaluated according to metrics designed to assess the quality of TSC data and its contribution to the performance and effectiveness of TSC customers. TSC will develop a means of using metrics to evaluate TSC performance over time, and each review will be assigned an owner, priority, start date, and projected end date.

31. In May 2005, the Government Accountability Office issued a report on U.S. passport fraud detection efforts and identified several weaknesses in those efforts, including that TSC neither provides consolidated terrorist watch list information to the State Department in a systematic manner nor routinely provides the names of other individuals wanted by federal and state law enforcement authorities. The Report indicated that the State Department sent a proposal on sharing watchlist information to TSC in January of 2005 and a written request outlining its needs for access to information on wanted persons in April 2005.

a. What steps has TSC taken to share with the State Department information from the consolidated watchlist and the FBI's database on wanted persons?

Response:

An MOU between the Department of State (DOS) and the TSC regarding the export of TSC data into the Passport Class System was signed by Assistant Secretary of State for Consular Affairs Maura Harty and by TSC Director Donna Bucella in late June 2005. The program was implemented on 7/25/05.

The FBI's database on "wanted persons" is managed by the FBI's CJIS Division, rather than by the TSC. In June 2005, the FBI began providing to DOS all NCIC "wanted persons" information derived from FBI files in order to enhance passport screening and fugitive apprehension. The FBI and DOS are in the process of completing an MOU to document this process. In addition, the FBI and DOS are attempting to coordinate the provision of access to non-FBI "wanted person" information in NCIC for passport screening purposes.

b. What, if any, obstacles prevent sharing this information, and when will the State Department have access to this information?

Response:

There are no obstacles to the sharing of this information. The TSC has been exporting Terrorist Screening Database (TSDB) data to DOS since the program was implemented on 7/25/05.

32. What is the average amount of time it takes to translate high priority counter-intelligence audio, which the Inspector General found is not always reviewed within 24 hours?

Response:

At present, the FBI does not collect this information. Based on the OIG report, we are conducting a complete review of our collection of language processing management data to ensure we capture this and other vital information.

33. I understand from your colleagues in the Bureau that real time translation is likely not possible, but they often speak of "near real time." Translating material on a near simultaneous basis could be critical to preventing an attack, just like listening to suspected criminals on a traditional wiretap can help officials to prevent planned crimes from being carried out. What are the realistic prospects for such material to be translated in something approximating real time?

Response:

Given the volume, velocity, and variety of information collected, near real-time translation of material is not likely absent advances in machine translation capabilities. Near real-time review of critical language material is possible through a combination of priority setting, selection tools, and rudimentary machine translation capabilities.

The FBI is not focused on moving from "near real time" review to "real time" review because it is far more efficient for a linguist to review the foreign language material after it has been recorded. The linguist is able to eliminate any "down time" (such as "dead air" time) by scanning the audio or text rather than listening to or reading the material as it is being produced. In addition, review is conducted in "near real time" because foreign language material is most often routed to the linguist electronically, typically as soon as the phone call or other event ends. Routing the work to the linguist, as opposed to sending the linguist to the collection site, allows the FBI to address even obscure languages quickly and enables a single linguist to process the work from several offices. This would not be possible if we were to place linguists physically at the site of collection to process material in "real time." "Near real time" may be as soon as the target hangs up the phone or up to 24 hours later, depending on the availability of resources proficient in the foreign language.

34. Your testimony states that the FBI can generally translate its high priority counter-terrorism audio within 24 hours. When the FBI misses that 24 hour target, what is average amount of time that it takes to translate high priority counter-terrorism material?

Response:

The FBI endeavors to review all of its highest priority Foreign Intelligence Surveillance Act (FISA) material within 24 hours of receipt and is generally successful in doing so. The OIG recently conducted tests in eight of the FBI's major translation centers and did find two instances in which material from the highest priority cases was not reviewed within 24 hours (a third instance noted by the OIG involved a negligible amount of material), but in both cases the material was reviewed within 48 hours.

35. The FBI modified its quality control guidelines in response to the July 2004 audit by the Inspector General. Those new guidelines took effect in December 2004. The July OIG report shows, however, that there is still no nationwide system in place to ensure that FBI field offices perform quality control reviews, or that they monitor the results of reviews. How can you explain this delay?

Response:

At the time of the OIG report, our quality control program had just been implemented and the first reports from that program were not available for OIG review. The OIG did acknowledge that after auditors had completed their field work the FBI provided "documentation showing that it had initiated a nation-wide tracking system and had used the new system to track the first quarterly report received in April 2005." The FBI continues to improve this program and expects to make further progress as we are able to hire and deploy additional personnel. These additional personnel resources will include Regional Program Managers and linguists, who will assist in improving quality control measures and in monitoring the field's compliance with these measures and with other foreign language program initiatives.

Questions Posed by Senator Feingold

36. Thank you for the additional information your office provided regarding the FBI's use of commercial data. When we met earlier this month, you told me that the FBI has contracts with commercial data brokers, but that agents search these databases only for particular information about individuals already under suspicion, and not to look for patterns of behavior that indicate an individual might be a terrorist. Is that a fair characterization?

Response:

That is generally a fair characterization. Commercial databases can be searched by FBI employees for information about individuals and groups in whom the FBI has a valid investigative interest. The FBI does not search commercial databases for patterns of behavior that might be associated with actions of terrorists.

37. Please provide the Committee with copies of the contracts that the FBI has entered into with commercial data brokers.

Response:

By letter to the Committee dated 4/18/05, we responded to a 3/31/05 letter requesting documents, including active FBI contracts with data brokers. In our response, we noted that on 4/7/05 Judiciary Committee staff received a detailed classified briefing on contracts DOJ and the General Services Administration (GSA) have with data brokers to obtain personal information for investigative purposes. Committee staff also received an unclassified briefing on 3/21/05 from DOJ and FBI officials regarding a recent ChoicePoint compromise, a portion of which addressed DOJ contracts with data brokers. As discussed during the 4/7/05 briefing, the FBI uses the services of Axciom, ChoicePoint, Dun and Bradstreet, iMAPdata, LexisNexis, Seisent (Accurint product), and Westlaw through contracts held by DOJ, GSA, and the Department of the Interior. DOJ provided to the Committee redacted copies of relevant DOJ contracts during the week of 4/11/05.

38. If the FBI begins to explore the application of data mining technology to commercial data, will you commit to informing the Committee about your plans?

Response:

As the FBI has indicated in previous written responses to this Committee, the FBI does not use public source providers to data mine or run "open-ended" searches for people who might fit a certain pattern. If the FBI should decide to run "open-ended" pattern searches, we will notify the Committee.

39. Please provide information, in classified form if necessary, regarding any reliance by the FBI on the use of pattern analysis technology or other statistical methods to analyze its own investigative files. Please detail the type of technology employed, the type of data subject to such analysis, any outside contractors involved in this type of analysis, and any guidelines governing such analysis.

Response:

If the term "pattern analysis technology" is used to mean the ability to enter into a computer system a series of general characteristics that operates over a broad set of data to automatically provide a list of those likely to be terrorists, the FBI neither has such a capability nor is seeking to develop one. The FBI does, however, use the IDW to conduct ad hoc and batch queries across documents stored as unstructured data (approximately 50 million documents stored in "flat files," which have no significant structure to permit the identification of data elements) and structured data (approximately 413 million documents containing structure that reveals data elements and permits extraction, transformation, and loading into a database). The set of searchable documents is growing through the addition of new sources of information from both FBI systems and those of other Federal organizations.

These capabilities are provided by commercial products that are integrated into IDW to provide search services, name processing services, and extraction, transformation, and loading services.

Search services.

Search services provided by Chiliad products operate over "unstructured" documents (such as text-rich messages, scanned documents, word processing files, and PowerPoint files), and over data extracted and loaded into Oracle databases. The Chiliad product will operate over data in any Open DataBase

Connectivity-compliant relational database management system. Data fusion takes place during indexing and search/analysis. The Chiliad technology suite uses various pattern matching techniques, including contextual searches, probabilistic searches, automatic concept recognition, named entity extraction, and a stemming algorithm.

Search services provided by Convera use Adaptive Pattern Recognition Processing technology. This technology allows investigators to perform searches for people who have aliases, name variants, or a variety of name spellings, and permits complex searches with complete flexibility in search terms, including any number of wildcards or patterns. Convera also permits the application of pattern recognition technology to search profiling. This technology allows users to register queries using a pattern recognition format, after which all new content flowing into the system is examined for matching patterns and/or wildcards in real-time and users are notified of matches.

Name processing services.

Applications provided by Language Analysis Systems are used to compute probabilities and associated confidence factors for male/female sex determination based on name, to compute probability that a given name is associated with each of 12 nationality groups, and to identify a set of closest matching names in an existing database of names. The computations of probable gender, nationality group, and closest matching names are achieved using pattern matching and statistical analyses of names based on extensive research and analysis of the linguistic and computational properties of names.

Extraction, transformation, and loading services.

IQ Insight is a data profiling tool that can be used to query database tables or flat files to identify patterns, including user-defined patterns (e.g., phone numbers, social security numbers, electronic mail message addresses, names, titles, company names and departments, dates, and addresses). IQ Insight is used to verify that the information in a particular field meets the range, format, and other characteristics expected for that information.

Several contractors assist with IDW maintenance: Scientific Applications International Corporation, Northrop Grumman Corporation - Information Technology Division, and Titan Systems Corporation assist with system operations and maintenance; Chiliad, Convera Corporation, and Informatica Corporation provide vendor support; EW Solutions, Mitretek Systems, and

Buchanan Edwards assist with security and data engineering; and SPAWAR, Eagan, McAllister Associates, Inc., provide program management support.

IDW is an FBI system, and all users must complete mandatory FBI Information Technology Security Awareness training. Users include FBI SAs and analysts, contract analysts serving in operational capacities, and detailees from other federal, state, and local agencies who have been verified as having an operational need for access. Multiple banners (FBI network and IDW) alert users to the restrictions on their use of the IDW system.

Requests to add data sources to IDW must include Privacy Impact Assessments (PIAs), which are reviewed by the FBI Office of the General Counsel (OGC). OGC's reviews of IDW PIAs are then reviewed by the FBI Information Policy Sharing Group, which must approve all sources of data hosted by IDW.

40. The Patriot Act authorized roving taps under the Foreign Intelligence Surveillance Act. That provision did not include an ascertainment requirement, as there is for roving taps under the criminal law. The criminal wiretap statute requires that for roving taps, "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted." 18 U.S.C. § 2518(11)(b)(iv). This ensures that when the order itself does not specify the facility to be tapped, innocent people's phone and computer conversations are not intercepted.

a. Would you object to including a similar ascertainment requirement for FISA roving taps? If your answer is "yes," please explain your reason(s).

Response:

As explained in more detail in the 5/24/05 letter to the Senate Select Committee on Intelligence attached as Enclosure E, the FBI would object to imposing that "ascertainment requirement" for FISA roving wiretaps. The proposed ascertainment requirement would deprive FBI investigators of necessary flexibility in conducting Section 206 roving surveillance. Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world, and are capable of engaging in detailed and extensive counter-surveillance measures. Adding the proposed ascertainment requirement might jeopardize the FBI's ability to conduct surveillance because, in attempting to physically ascertain where the target communication will take place, FBI agents would run the risk of being exposed to sophisticated counter-intelligence efforts.

In addition, the proposed ascertainment requirement would impose significant, unwarranted burdens in cases that are already difficult because of actions by the target that have the effect of thwarting the surveillance. Generally, communications intercepted by criminal Title III surveillance are monitored and minimized contemporaneously by law enforcement personnel. In contrast, communications intercepted pursuant to FISA are generally not contemporaneously monitored. FISA surveillance generally involves after-the-fact review pursuant to mimimization procedures approved by the FISA Court (FISC) that limit the acquisition, retention, and dissemination of information about United States persons (thus protecting the privacy of innocent individuals). Under FISA, regardless of whether the surveillance is pursuant to a section 206 order, conversations of "innocent people" are minimized (i.e., not retained in any easily retrievable manner), unless they are talking to or about the authorized target of the surveillance.

Presently, Section 206, together with the practicalities of how surveillance occurs (as discussed below), provides sufficient safeguards to ensure that an innocent person's telephone and computer conversations are not inadvertently intercepted. The target of the roving surveillance must be identified or described in the FISA application with sufficient particularity to permit the FISC to conclude that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Section 206 roving surveillance can be ordered only if the FISC finds, after having determined that the requirements for FISA electronic surveillance have been met, that the actions of the specified target may have the effect of thwarting the surveillance. If the government can demonstrate that to the satisfaction of the FISC, it then obtains a secondary order that can be served on any provider of a facility subsequently determined to be used by the target. As a practical matter, the FBI determines that the target is using a particular facility before it serves the order and begins monitoring the new facility. That determination is, however, very different from a requirement that the FBI must have observed the target near to or on the new facility before it can monitor the resulting communication.

b. Please explain, in the context of a FISA roving tap, how agents make the decision which facilities to tap. If agents do not ascertain that the target is using a particular facility, how do they decide which facility to tap? How do they decide when to start listening in on the tap?

Response:

This question suggests that there may be a misapprehension about how "roving FISA surveillance" under Section 206 is conducted.

When the FBI determines that the target's actions may have the effect of thwarting surveillance (either by virtue of the target's own practice of switching providers or because the target works for an entity that has an established practice of engaging in tradecraft that thwarts surveillance), the FBI may apply for "roving" electronic surveillance authority. In that event, the court's order would require the known telephone service provider to facilitate the surveillance and would provide the FBI with another order that requires a "specified person" to facilitate the surveillance of the target. The FBI can then serve that second order on any cellular telephone service provider after the FBI has confirmed that the target is using or about to use a new facility, i.e., that he has "roved." Currently, a notice is filed with the FISC identifying the new facility after an order is served on the new provider.

41. Do you agree that if Congress were to grant the FBI the administrative subpoena authority that you sought at the hearing, the FBI would be highly unlikely to seek a Section 215 order or a National Security Letter ever again? If your answer is no, please describe the circumstances under which the FBI would seek a Section 215 order or an NSL rather than issue an administrative subpoena.

Response:

We do not agree that obtaining administrative subpoena authority would render section 215 orders or National Security Letters (NSLs) obsolete. Generally, the FBI will use the most effective and time-efficient tool available for an investigation, taking into account the type of record sought and our knowledge of the custodian of those records. Administrative subpoena authority would clearly provide a mechanism for obtaining relevant information in national security investigations quickly and without significant expenditure of personnel resources. Although administrative subpoenas might well become the FBI's national security tool of choice, they would not become its only tool. For example, the FBI may well choose to seek a Section 215 order in a very sensitive investigation in which the added imprimatur of a court order to maintain the secrecy of the order is needed (e.g., past experience with the document custodian suggests a lack of care with administrative requests). The FBI may also use a 215 order if it is seeking records that are particularly sensitive, making review by a court before seeking the documents appropriate. The FBI's experience with criminal administrative subpoenas shows that criminal investigators do not limit themselves to one tool, but instead use whatever tool most effectively and efficiently obtains the needed information. We expect our SAs handling national security investigations to exhibit the same initiative in their investigations.

42. Thank you for your prior responses to questions about the operations of the Terrorist Screening Center (TSC). You explained in those responses that TSC has hired a Privacy Officer to help address complaints about the operation of the TSC watch lists. Please explain the role of the Privacy Officer. Who does the Privacy Officer report to? Does the Privacy Officer have full clearance to review all TSC data?

Response:

The TSC Privacy Officer is formally supervised by the TSC Director, and additionally reports informally to the TSC Chief of Staff to ensure proper coordination of assignments and other matters. The Privacy Officer is responsible for establishing internal policies and procedures to ensure the TSC is in compliance with laws and policies related to the handling of personal information, and for recommending additional policies to ensure that appropriate privacy protections are afforded even in the absence of regulation. The Privacy Officer has full clearance to access all data maintained and used by the TSC in the performance of its mission.

43. The June Inspector General report evaluating TSC identified problems with the completeness and accuracy of the watch list data, in terms of both omitting known terrorists and including inaccurate information about individuals. What steps is the TSC taking to rectify this problem?

Response:

The TSC is using sophisticated database queries to check for data anomalies, performing record-by-record reviews of the data known to be the most likely to contain inaccuracies, and employing sophisticated custom software to evaluate incoming data against 44 business rules in order to ensure errors do not enter the database.

44. Would the FBI be willing to allow cleared staff of the Judiciary Committee to visit the TSC to better understand how the watch list process works, how names are added and removed from the list, and how TSC interacts with other agencies?

Response:

On various occasions, the FBI has invited Judiciary Committee members and staff to tour the TSC and obtain a briefing concerning its activities and evolution. We would be pleased to arrange such a visit at the Committee's convenience.

45. Please provide a list of each federal government agency, department or other entity that relies on the TSC to screen individuals, and the purpose of each screening program. Please include programs in which the government agencies run the names of private sector employees against the watch list.

Response:

The law enforcement components of federal agencies rely on the TSC to screen individuals through the TSDB to identify known or appropriately suspected terrorists, and to provide this information to them on a real-time basis. The initial inquiry by federal law enforcement officials is most often precipitated by a "hit" in the NCIC's VGTOF. The majority of federal encounters in which the TSC is engaged are initiated by the National Targeting Center, which is managed by DHS.

The TSC does not currently run the names of "private sector employees" against the watchlist or any other TSC database unless, of course, they are the subjects of the law enforcement encounters described above. The establishment of programs to support private sector screening is a task for which the DHS is responsible. When those programs are established, the TSC will provide appropriate mechanisms to ensure these screening opportunities are managed properly.

46. Please provide information about the state and local agencies, departments or other entities that rely on the TSC to screen individuals, and the purposes for which they do so.

Response:

All state and local law enforcement agencies with NCIC access rely on the TSC's TSDB and the NCIC system to identify potential terrorism subjects.

The TSC is a multi-agency organization established under the authority of Homeland Security Presidential Directive 6 to ensure that the names of known or suspected terrorists collected by various U.S. Government agencies are merged into one consolidated list and appropriately shared with federal, state, local, territorial, tribal, and consular authorities, as well as with certain foreign governments. Participants in the TSC include the ODNI, DOJ, DHS, DOS, DoE, and Department of the Treasury. TSDB information is exported to multiple supported systems, including the NCIC's VGTOF. State and local law enforcement authorities are able to query VGTOF for operational direction concerning positively identified known or appropriately suspected terrorists on a "real-time" basis. The FBI's Terrorist Screening Operations Unit (TSOU)

coordinates the operational and investigative response to these inquiries with the appropriate JTTF, which includes representatives from the intelligence community and from the federal, state, and local law enforcement communities. The JTTF conducts liaison with the encountering agency. The TSC also notifies the North American Aerospace Defense Command (NORAD) and the Federal Air Marshal Service (FAMS) of positive encounters during TSC's airline screening process. NORAD is alerted to this information to provide them an opportunity to monitor "Selectee Flights," and FAMS is alerted to permit them to schedule Air Marshals on all "Selectee Flights," making better use of limited resources. These processes have been developed to address gaps within the overall terrorist screening effort and to improve the flow of terrorism-related information.

The ability of the TSC to identify, collect, review, and analyze intelligence from encounters with known or appropriately suspected terrorists increases the effectiveness of the FBI's overall terrorism intelligence base. Daily, this information is shared by the TSC's Tactical Analysis Unit with the FBI's FIGs, which include representatives from the FBI field offices in which they reside and may also include representatives from intelligence agencies and federal, state, and local law enforcement agencies. Through these efforts and those noted above, the TSC has assisted in greatly improving the flow of information between the FBI and state and local law enforcement agencies.

47. There have been reports that FBI agents registered serious concerns about interrogation techniques they witnessed officials from other agencies or departments employing at Guantanamo Bay.

a. When were these concerns brought to your attention?

Response:

Director Mueller does not have a specific recollection as to when he first received this information, but believes that by early 2002 he had determined that FBI Agents participating in interviews overseas should follow FBI protocols.

b. What steps has the FBI taken within the Administration to oppose the use of coercive interrogations?

Response:

The FBI has clearly communicated its view that rapport-building interview techniques are more effective than coercive or other aggressive techniques.

ENCLOSURE A

QUESTION 11b

SENTINEL STATEMENT OF WORK

UNCLASSIFIED
FOR OFFICIAL USE ONLY

Version 2.1
5 Aug 2005

SENTINEL
STATEMENT OF WORK

FOR OFFICIAL USE ONLY

UNCLASSIFIED

SOW To Be Determined (TBD)/To Be Reviewed (TBR)/To Be Supplied (TBS) Table

Seetion	TBD/TBR/TBS	Closnre Plan
5.5.3	Identify the number of training locations.	Offeror closes with proposal submission (based on the proposed training approach).
8	Contractor to provide base period length, Phase durations and end date as part of the proposal.	Offeror closes with proposal submission.
9.1-1, 18.81	**Delivery Acceptance Review deliverable 9.1-1**	Offeror closes with proposal submission.
9.2	Contractor to supply CLIN durations and start and end dates as part of the proposal.	Offeror closes with proposal submission.
11.3	Need date for test data	Offeror closes with proposal submission.
15.5.1	Usability Standards	Offeror closes with proposal submission.
15.7	Workspace -number of spaces to be determined.	Offeror closes with proposal submission.

TABLE OF CONTENTS

1. Acquisition

This Statement of Work (SOW) describes the Federal Bureau of Investigation's (FBI's) requirements for SENTINEL. The contractor shall be responsible for furnishing all personnel, facilities, equipment, material, supplies, support and management and shall perform all functions necessary to design, develop, integrate, test, deploy, operate and maintain SENTINEL as set forth in the SOW and the SENTINEL System Requirements Specification (SRS). This SOW is intended for use with the documentation listed in SOW Section 3.0, Applicable Documents. All of the requirements in the SRS, whether specifically referenced or not in the SOW, shall apply to the contractor's deliverable services and service performance.

2. Background and Objectives

2.1 Background

The Federal Bureau of Investigation (FBI) is completing the building and deployment of several infrastructure systems that modernize its IT capabilities. Referred to as the Trilogy Program, this FBI initiative consists of the following interrelated components:

- The Information Presentation Component (IPC) encompasses hardware and software within each office to provide each employee with a current desktop environment and equipment.
- The Transportation Network Component (TNC) is composed of high-speed connections linking the offices of the FBI.
- The User Applications Component (UAC) will include SENTINEL enhancing each employee's ability to access, organize, and analyze information.
- The Enterprise Operations Center (EOC) is the FBI's infrastructure management center that oversees, monitors, and manages the Trilogy assets.

The IPC, TNC and EOC efforts are complete. The operational system is referred to as FBINet.

The FBI currently uses paper as their system of record while electronically managing the information. The current methods of managing case file information are outdated and inefficient. In order for the FBI to more effectively perform its mission, the case management system must be upgraded to utilize enabling information technologies.

SENTINEL will transform the way the FBI does business, allowing the Bureau to move from a primarily paper-based case management system to an electronic system of records. SENTINEL will leverage technology to reduce redundancy, eliminate bottlenecks and inefficiencies, and maximize the FBI's ability to use the information in its possession. SENTINEL will be an integrated system that will support the processing, storage, and management of information to allow the FBI to more effectively perform its investigative and intelligence operations.

The SENTINEL acquisition continues the FBI's transformation to an enterprise-wide automated case management system that began with the Virtual Case File (VCF) Pilot.

2.2 SENTINEL Acquisition Objectives

The objectives of the SENTINEL acquisition are:

- Objective 1: To incrementally design, develop, integrate, test, and implement a set of capabilities that meets the requirements outlined in the SENTINEL System Requirements Specification with operationally useful increments delivered approximately every 12 months. At a high level the delivered system shall:
    - Implement paperless case management and workflow capability (Priority 1).
    - Provide a single point of entry for investigative case management.
    - Implement electronic records management.
    - Implement a new and improved Bureau-wide global index for persons, organizations, places, things, and events.
    - Facilitate information sharing among law enforcement agencies and the intelligence community.

- Objective 2: To efficiently and cost effectively transition users and data to the new system. Transition steps include:
    - Retiring FBI legacy case management systems (or elements of them) as rapidly and efficiently as possible.
    - Timely, accurate and efficient data migration from legacy systems.
    - Transition of all users to the new system as services and data become available.

- Objective 3: To establish an Organizational Change Management (OCM) strategy enabling users to learn new behaviors, skills, and business processes through robust training and outreach programs.

- Objective 4: To enhance user interaction with SENTINEL, combining new and legacy components through intuitive human system interfaces presenting actionable data and items of interest to the user as requested or via data rules.

- Objective 5: To provide the FBI with a flexible and extensible IT infrastructure for SENTINEL that accommodates incremental composition and integration of capabilities that achieve an event driven Service Oriented Architecture (SOA).

- Objective 6: To exploit and utilize to the maximum extent possible government owned and/or commercial-off-the-shelf (GOTS/COTS) components. The Government desires a modular, component-based approach leveraging standards-based protocols and the best of commercially available IT technologies.

- Objective 7: To successfully accredit each Phase beginning with the first deployment including:
    - Information assurance Approval to Operate at the level specified in the SRS
    - Recordkeeping certification and Approval to Operate as applicable to each Phase

- Objective 8: To operate and maintain each deployed Phase at the levels specified in the Government approved[1] contractor generated Service Level Agreements (SLAs).

[1] The Service Level Agreement will be generated as part of the Phase development activity by the contractor. The Government is the approval authority.

- Objective 9: To transition operations and maintenance of the system to the FBI's Information Technology Operations Division (ITOD) at the completion of the final operations and maintenance period (approximately two years after the final Phase deployment) or earlier at the request of the Government.

3. Applicable Documents

A list of documents referenced throughout the SOW is presented in sections 3.1 and 3.2. Compliance documents shall be complied with. Guidance documents are provided for reference.

3.1 Compliance Documents

a) FBI SENTINEL Configuration Management Plan V1.1, 20 July 2005
b) FBI SENTINEL Risk Management Plan V1.2, 8 July 2005
c) FBI Information Technology (IT) Life Cycle Management Directive (LCMD) Version 3.0 draft as of 30 June 2005
d) FBI SENTINEL System Requirements Specification (SRS) V1.1, 29 July 2005
e) FBI Certification and Accreditation Handbook V2.1, 1 Jun 05
f) National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M 1995, with Changes 1 (1997) and 2 (2001)
g) FBI Electronic Recordkeeping Certification Manual V1.0, 30 April 2004
h) NDIA PMSC Surveillance Guide - ANSI/EIA Standard 748 (current version at time of solicitation)
i) NDIA PMSC Internet Guide - ANSI/EIA Standard 748 (current version at time of solicitation)
j) Commercial Delivery Instructions J. Edgar Hoover (JEH) FBI Building and Washington Field Office (WFO) dated 27 Dec 2000
k) ITOD Data Unit, Equipment Installation Standards, 10 May 2005
l) ITOD Data Unit, Equipment Installation Standards (Clarksburg, West Virginia), 12 May 2005
m) Software Update Services (SUS) Patch Management Process, 20 April 2005
n) FBI SENTINEL Incremental Development Plan V1.0, 29 July 2005
o) FBI SENTINEL CONOPS, 25 July 2005
p) FBI Enterprise Architecture (EA) Target Architecture Report V1.0, 31 May 2005
q) FBI SENTINEL Test and Evaluation Master Plan (TEMP) V1.1, 22 July 2005

3.2 Guidance Documents

a) FBI SENTINEL Program Management Plan V1.0, 22 July 2005
b) Technical Reference Model, V 0.51, 1 July 2005
c) Oracle Database Element Naming Standards V1.1, 24 September 2001
d) Oracle Database Development Standards, Version 1.0, 14 April 2003
e) Oracle Database Security Marking Standards V1.0, 26 March 2002
f) Oracle Database User Audit Requirements Specification, Version 1.3, 28 Sep 2001

4. Scope

The task order scope is worldwide and includes efforts related to four CIO-SPi-2 Task Areas as follows:

- CIO-SP2i Task Area 3. IT Operations and Maintenance. (Objectives 8 and 9 above)
- CIO-SP2i Task Area 4. Integration Services (Objectives 1, 2, 3, 4, 5, 6, and 7 above)
- CIO-SP2i Task Area 5. Critical Infrastructure Protection and Information Assurance (Objectives 1 and 7 above)

- CIO-SP2i Task Area 9. Software Development (Objectives 1, 5 and 8 (post Full Operational Capability) above)

5. Specific Tasks

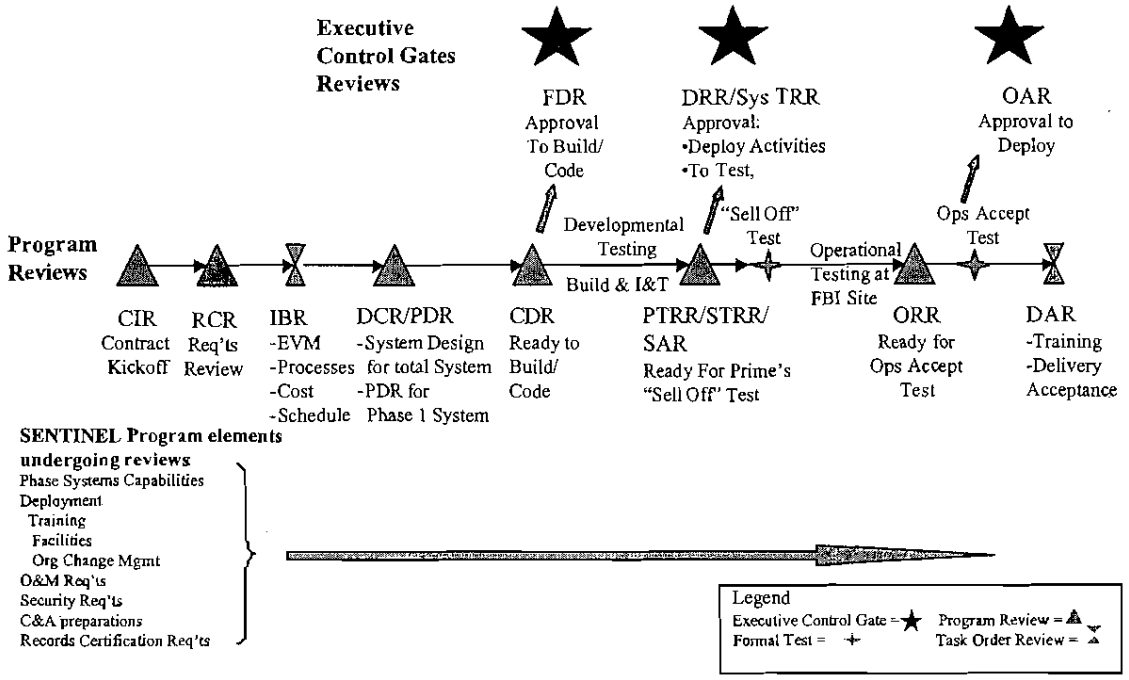
The Government's objective is to receive a sustainable and maintainable delivery approximately every 12 months (Operational Readiness Review from FBI IT LCMD). Each delivery shall constitute an incremental Phase. Each Phase, when deployed, represents a standalone set of capabilities that can be added to by subsequent Phases to achieve the SENTINEL Objectives. Phases may overlap each other, e.g., Phase 1 may be in system development and test while Phase 2 is in system design. SENTINEL capabilities are established in the System Requirements Specification (SRS) and CONOPS. The Ineremental Development Plan eontains the phase content description.

A delivery is considered accepted with installation and training at all operational locations and the successful completion of site acceptance testing, records management certification, the achievement of Approval to Operate (or an Interim Approval to Operate), and a successful Operational Acceptance Review (ref. FBI IT LCMD). This delivery acceptance will be the focus of a program-level review entitled Delivery Acceptanee Review (DAR). The DAR shall include confirmation of all contractor work products provided to the Government for the delivery.

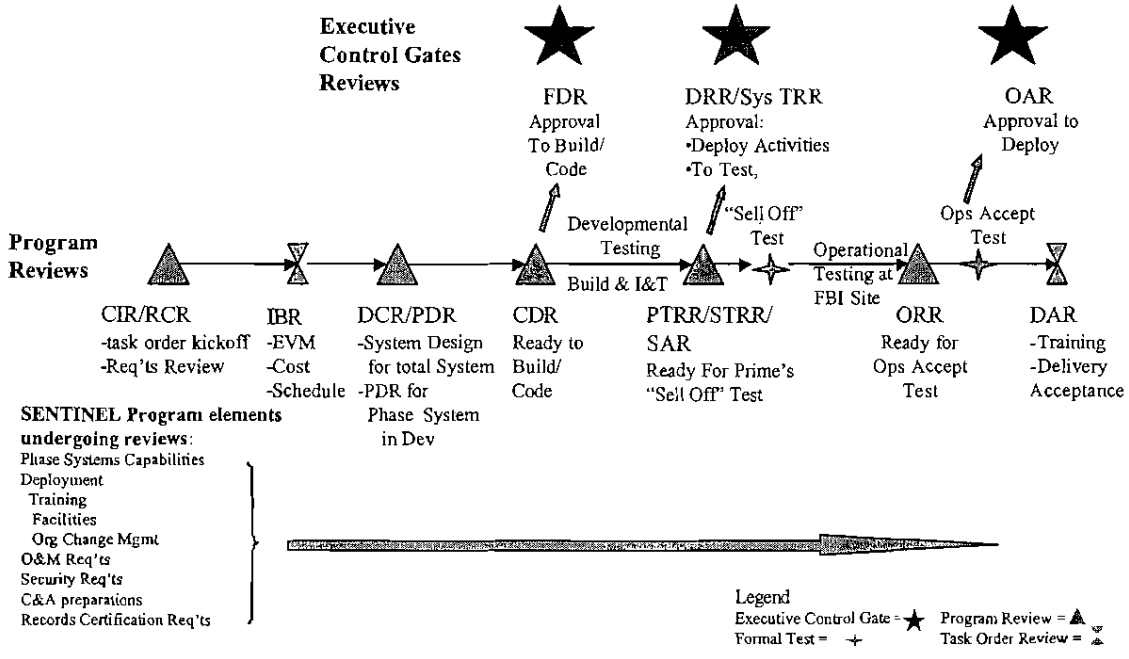
SENTINEL capabilities are established in the System Requirements Specification (SRS) and CONOPS. The Incremental Development Plan contains the Phase content descriptions.

The Phase 1 Development and Deployment and Phase 1 Organizational Change Management shall comprise the basic task order. Phases 2 – 4 Development and Deployment, all Operations and Maintenance, and Phase 2 – 4 Organizational Change Management shall be priced task order options.

The Government has applied the following tailoring to the FBI IT LCMD Control Gates and Program Reviews for Phase 1:



The Government has applied the following tailoring to FBI IT LCMD Control Gates and Program Reviews for Phases 2-4:



The SENTINEL Prime Contractor shall conduct the Program Reviews. The SENTINEL Government Program Management Office will conduct the Control Gate Reviews using an executive summary of the material provided by the contractor at the Program Reviews.

Additionally, in accordance with the FBI IT LCMD process, as Phases 2-4 constitute priced task order options; the Government Program Management Office will obtain separate Acquisition Plan Review, FBI

IT LCMD Control Gate 2, approvals prior to task order option awards for CLINs 2, 3, and 4 (notional, section 9.2)

5.1 Task 1-Contract-Level and Task Order (TO) Management

5.1.1 Task 1 Subtask 1-Contract-Level Program Management

The contractor shall provide the technical and functional activities at the contract level needed for program management of this SOW. The contractor shall also provide the centralized administrative, clerical, documentation and other related functions.

Performance of this subtask support shall be included for all subtasks within this task order as NotSeparately Priced (NSP) Items.

5.1.2 Task 1 Subtask 2-Task Order Management

The contractor shall manage all effort resulting in the delivery of SENTINEL. The contractor's management effort shall include administration, program controls, product effectiveness, data and configuration management, risk management, subcontract management, and security management.

The contractor shall define, execute, and manage SENTINEL incremental Phases' development and deployment through the application of an Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) approach. Additionally, the IMP and IMS shall reflect the FBI IT LCMD requirements for SENTINEL Program and Control Gate Reviews. The contractor shall plan and execute against a set of processes tailored for this task order.

The contractor shall establish a Work Breakdown Structure (WBS) for SENTINEL down to at least Level 6 in order to fully describe the contractor's work effort. Consider the SENTINEL program as Level 1. Additionally, no labor driven non-level of effort work packages shall exceed 30 calendar days. The WBS numerical framework shall be applied to the IMP, IMS and cost reporting system that will establish a single common framework across the program for management, tracking and reporting. The numerical framework directly links the WBS with the IMP, IMS and cost which will provide a single SENTINEL reporting framework.

The contractor shall ensure that there is a single set of implementing processes used by all including subcontractors in carrying out the tasks and activities contained in the IMP, IMS and SOW Tasks 1, 2, 3, 4 and 5. Utilization of a single set of implementing processes shall be verified at the Contract Implementation Review.

The contractor shall: establish and execute the technical approach; organize resources; and establish and execute management controls to ensure the cost, performance and schedule requirements of the task order are met.

5.1.2.1 Earned Value Management System (EVMS) Implementation

The contractor shall establish an earned value management system immediately after contract award. The contractor shall present their earned value management system and their earned value baseline (EVMS Report) to the Government for review, comment, and the Contracting Officer's approval as part of an Integrated Baseline Review (IBR). The IBR shall occur no later than 14 calendar days after the start of the Requirements Clarification Review (RCR). The contractor's earned value management system shall comply with all of the common criteria contained in ANSI/EAS Standard 748 (current version at the time of solicitation).

The contractor shall manage and report against the established earned value management system and the established earned value baseline beginning immediately after contract award. This earned value

management and earned value reporting shall continue through the completion of the contract. The contractor shall prepare and submit a status report to the Contracting Officer at least monthly (Gregorian calendar) that details the contractor's most recent performance against the established earned value baseline. The monthly reports shall clearly distinguish between performance against the earned value baseline as a whole and performance against the portions of the earned value baseline that are not related to work packages measured using a Level of Effort (LOE) methodology.

In addition to the common criteria contained in ANSI/EAS Standard 748, the contractor's earned value management system, the contractor's earned value baseline, and the contractor's monthly earned value status reports shall comply with the detailed requirements contained in SOW Attachment-1, Earned Value Management System Requirements of this Statement of Work. In the event that there is ambiguity and/or conflict between ANSI/EAS Standard 748 and Attachment-1, the requirements of Attachment-1 shall prevail.

5.1.2.2 Risk Management Program

The contractor shall perform risk management in accordance with its corporate policy and the requirements contained in the FBI SENTINEL Risk Management Plan.

The contractor shall implement a formal risk management process that encompasses: risk management planning and budgeting; risk identification, assessment, and analysis; risk contingency planning; and risk monitoring and control (including decision procedures for escalation and exercising contingency options).

5.1.2.3 Configuration Management (CM) Program

The contractor shall perform configuration management in accordance with its corporate policy and the requirements contained in the FBI SENTINEL CM Plan and the FBI IT LCMD.

The contractor shall implement a formal CM program that includes Configuration Identification, Change Management, Configuration Status Accounting, Audit, and Release Management. The contractor shall comply with all Government CM processes and procedures as outlined in the Government's SENTINEL CM Plan. The contractor shall perform all CM activities until contract completion. The contractor shall ensure that all subcontractors and vendors comply with the CM requirements levied by the Government's CM Plan and this SOW.

5.1.2.4 Quality Assurance (QA) Program

The contractor shall perform quality assurance to include activities such as defect tracking, root cause analysis, peer reviews of all development artifacts, and appropriate levels of testing in accordance with corporate practices and the requirements of this SOW.

5.1.2.5 Security Management (facilities and personnel)

The contractor shall perform security management in accordance with the SOW Attachment-2 Contract Security Classification Specification (DD Form 254) and the additional security requirements outlined in this SOW.

5.1.3 Task 1 Subtask 3-Data Management Program

The contractor shall implement and maintain a single data management program that contains the data and information used in managing the contractor's SENTINEL program. The contractor shall provide the Government direct insight into the current program state through a data management repository. This data management repository shall be on-line and accessible from the Government program office(s) and spaces at the contractor's facility. The data repository shall include all materials generated during the program execution. Data shall include, but is not limited to, activity artifacts and results from: requirements

management and verification, architecture management, configuration management, quality assurance, risk management, earned value management, and program schedule data.

The contractor shall provide training and training materials on how the Government can achieve insight into the state of program through the data management program. The training shall cover each of the management support tools the Government shall be able to access through the data management program. For cost estimating purposes, the contractor shall assume 4 semi-annual training sessions, to be held in Government program office spaces, with the first training session consisting of 12 Government-identified personnel, and for up to 6 Government-identified personnel in each remaining session.

5.1.4 Task 1 Subtask 4-In Progress Review Support

The contractor shall provide a monthly status report containing the status of all ongoing SOW tasks. Topics to be addressed include: the Earned Value, schedule, risks, program and risk management metrics, quality assurance, configuration management, data deliveries, 6month staffing forecast, and security management applied to the task order. The contractor shall participate with the Government in formal monthly reviews and informal weekly status reviews. Contractor participants in the formal monthly reviews shall be empowered to aceept and make commitments on behalf of the contraetor, within the limits of the SENTINEL contract.

5.1.5 Task 1 Control Gates and Program Reviews

The following control gates and program reviews (ref. FBI IT LCMD) are applicable to this activity:

- Contract Implementation Review (within 14 calendar days of contract award)
- Integratcd Baseline Review (within 14 calendar days of the requirements clarification review)(described in Attachment 1)
- In-Progress Review (monthly) (deseribed in SOW paragraph 5.1.4)

5.1.6 Task 1 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.2 Task 2-SENTINEL Systems Engineering and Architecture

Thc contractor shall implement the systems engineering and architecture activities required to precede and support phase level planning, design, development, integration, test, deployment, and operations and maintenance activities.

5.2.1 Task 2 Subtask 1-SENTINEL Systems Engineering Management

The contractor shall implement a tailored systems engineering approach for defining, designing, developing, integrating, testing, and deploying SENTINEL's capabilities in incremental Phases. This approach shall be based upon the contractor's established Systems Engineering Methodology and implementing processes. The contractor shall include architecture development, system development, integration and test, and deployment as part of its systems engineering approach. This approach shall be described in its Systems Engineering Management Plan and be visible in the Integrated Master Plan, Integrated Master Schedule, and reflected in the Work Breakdown Structure.

The contractor shall support the FBI IT LCMD control gates and project reviews for the SENTINEL program and its incremental Phases implementation.

The contractor shall develop and utilize a specification hierarchy in determining and producing a necessary set of technical documents that describes the SENTINEL technical baseline. This technical baseline shall be updated upon commencing of a Phase's deployment to the FBI Enterprise. The contractor specification

hierarchy shall commence with a SENTINEL System Specification that validates the SRS and translates its functional and performance requirements into system specifications.

The contractor shall prepare and maintain a system specification in response to the Government SRS. The Government will retain management of the SENTINEL SRS.

The contractor shall manage all requirements and specifications for SENTINEL below the SRS level. The contractor shall allocate system requirements to capabilities. The contractor shall identify the system requirements that will be satisfied in part or completely at the end of each of Phase. The contractor shall determine the verification method of each system requirement. For those system requirements developed and delivered incrementally (i.e., in more than one Phase), the contractor shall indicate the level of system requirement capability by Phase and the method of verification in each Phase.

As noted in the SRS, Sentinel will require information sharing with systems classified higher than Collateral Secret (e.g., with Intelligence Community) and with systems at a lower classification level (e.g., state and local law enforcement). This will require the offeror to address Controlled Interface Guards (see, e.g., http://www.dtic.mil/whs/directives/corres/html2/d46305x.htm). The specific networks and data types to be addressed at both the high side and low side are to be determined, but the offeror will have to address this capability in the proposed system design.

For all system performance requirements (e.g., availability, throughput, responsiveness of the system), the contractor shall develop, document, and maintain planned technical performance profiles, and associated out-of-band reporting profiles, that span the entire SENTINEL development. As actual data becomes available, the contractor shall include the actual values in the profiles. The contractor shall identify the system performance requirements that will be satisfied in part or completely at the end of each Phase.

The contractor shall develop and utilize a system level Test and Evaluation Master Plan (TEMP) that accommodates SENTINEL evolution across its Phases and with an evolving FBI Enterprise. The Government TEMP provides a framework of specific areas that should be addressed in the contractor's SENTINEL TEMP. The contractor TEMP shall be consistent with the test approach outlined in the Government TEMP. The TEMP shall also include the contractor's integration and test facility that supports its approach, its test processes, Certification & Accreditation (C&A) approach, records management certification approach, and test data requirements.

SENTINEL has been designated a National Security System. As such, it must meet requirements set by National Information Assurance Partnership (NIAP) and National Security Telecommunications and Information Systems Security Policy (NSTISSP)-11. (General information is available at: http://niap.nist.gov/cc-scheme/nstissp-11-faqs.pdf). There are two general cases that may be applicable to the SENTINEL program and that the contractor shall account for in their design and development activities:

1. If an approved U.S. Government protection profile exists for a particular technology area, but no validated products that conform to the protection profile are available for use, the acquiring organization must require, prior to purchase, that vendors submit their products for evaluation and validation by a NIAP laboratory or Common Criteria Recognition Arrangement (CCRA) laboratory to a security target written against the approved protection profile or acquire other U.S.-recognized products that have been evaluated under the sponsorship of other signatories to the CCRA.

2. If no U.S. Government protection profile exists for a particular technology area and the acquiring organization chooses not to acquire products that have been evaluated by the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) or CCRA laboratories, then the acquiring organization must require, prior to purchase, that vendors provide a security target that describes the security attributes of their products, and that vendors submit their products for evaluation and validation at a Designated Accrediting Authority (DAA)-approved Evaluation

Assurance Levels (EAL). Robustness requirements, mission, and customer needs will together enable an experienced information systems security engineer to recommend a specific EAL for a particular product to the DAA. In addition, the organization should file the necessary for a Deferred Compliance Authorization (DCA) (see FAQ #12 under Policy Information and Guidance http://niap.nist.gov/cc-scheme/nstissp-11-faqs.pdf).

In support of the delivery of a service-based solution, the contractor shall recommend to the Government an SOA governance approach. SOA Governance addresses the technical and business aspects of using and deploying services, and provides a review process to ensure that services are managed throughout their lifecycle. This requires appropriate definition of the procedures and policies to be complied with when making a service available to SENTINEL and/or to the Enterprise, and when any change is proposed to an approved service. The proposed Governance approach should address who is allowed to publish a service to the registry, establish the release procedures, and determine the approval and certification process for designs, standards and security policies. It should propose how to perform governance validation before allowing services to be published and how the FBI should follow that up by continued policy checks during use. The contractor shall participate in the governance process, once approved, as required by the process in the deployment of SENTINEL.

The contractor shall support the Government certification and accreditation process defined in the FBI Certification and Accreditation Handbook. This includes preparation for and support of Certification and Penetration Test and Evaluation as well as support to recurring Security Test and Evaluation once the system is operational.

The contractor shall support the Government Records Management Certification process defined in the FBI Electronic Recordkeeping Certification Manual.

The contractor shall support Government Independent Verification and Validation (IV&V) activities. The IV&V activities include monitoring the design, development and test, implementation and integration of SENTINEL. The Government IV&V activities are scoped as monitoring and oversight.

5.2.2 Task 2 Subtask 2-SENTINEL Architecture Management

The contractor shall develop, document, and maintain a SENTINEL architecture that (1) permits the incremental implementation and deployment of functional capabilities, (2) is scalable, flexible, and modular, and (3) leads to an easy to use system that users can access through the FBINet. The contractor shall conduct trade studies as required to define the architecture and to determine hardware and software.

The contractor shall develop a SENTINEL Target Architecture, with phased increments, that achieves SRS capabilities in deployable standalone Phases that can be added to by subsequent Phases to expand capabilities. Each Phase shall have its own architecture representation establishing the set of SENTINEL SRS capabilities that will be delivered.

The SENTINEL Target Architecture shall be compatible with and address the intent depicted in the FBI EA Target Architecture Report to the maximum extent possible. The contractor shall develop an architecture that conforms to the Government TRM to the extent practical. The contractor shall identify planned deviations from the TRM to the Government.

The contractor shall develop, model, document, and maintain materials sufficient to describe the architecture and business-driven performance criteria throughout the life of the system to include the development of business scenarios to validate the integrity of architecture. Performance analyses shall include the impact of implementing SENTINEL on FBINet.

5.2.3 Task 2 Control Gates and Program Reviews

The following control gates and program reviews (ref. FBI IT LCMD) are applicable to this activity:

- Requirements Clarification Review (2 weeks after CIR for Phase 1, in conjunction with CIR for Phases 2-4)
- Design Concept Review (in conjunction with Phase PDR)

5.2.4 Task 2 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.3 Task 3-Phase Design, Development, Test, Implementation, and Integration

The contractor shall eonduct all activities necessary to design, develop, integrate, test and deploy an incremental Phase that provides a set of defined capabilities and implements and integrates them with the existing FBI infrastructure.

The contractor shall create and maintain plans for Phase transition, deployment, and installation.

The contractor shall support the Government Certification and Accreditation process defined in the FBI Certification and Accreditation Handbook.

The contractor shall support the Government Records Management Certification process defined in the FBI Electronic Recordkeeping Certification Manual.

The contractor shall support Government Independent Verification and Validation (IV&V) activities. The activities include monitoring the design, development and test, implementation and integration of SENTINEL. The Government IV&V activities are scoped as monitoring and oversight; no independent testing of the system is planned as part of IV&V.

Support to Government testing includes: providing access to a correctly configured and documented system, keeping the system operational, providing access to all requested documentation; operating the system; performing the procedures during security testing and certification testing, and answering questions including showing system and software configuration details. The contractor shall also be required to establish (and remove at the completion of testing) test accounts (both general and privileged) as required in the test plan and procedures.

5.3.1 Task 3 Subtask 1-Phase Design

The contractor shall perform IMP and IMS engineering activities to ensure that each Phase satisfies the requirements allocated to it. The contractor shall decompose Phase requirements to the lowest level to effectively and efficiently complete the Phase detail design activities. The contractor shall create and maintain a verification matrix of the Phase's system level requirements.

The contractor shall develop, document, and maintain all internal interface requirements including the Document Creation Ingest Specification identified in the SRS.

The contractor shall develop, document, and maintain the SENTINEL side of all external interface requirements in conjunction with the parties responsible for other systems.

The contractor shall provide justification for the use of selected COTS products and any proposed custom development.

The contractor shall conduct all design activities necessary to create, maintain, and deploy each Phase (includes the underlying data) such that each Phase meets all system requirements, security and records management accreditation requirements and attains an Approval to Operate.

5.3.2 Task 3 Subtask 2 Phase Development and Test

The contractor shall acquire or develop all hardware and software components required to implement the approved Phase design. The contractor shall assemble, configure, integrate, and test all software and hardware components that are part of the Phase design in preparation for system level testing.

The contractor shall create and maintain Phase test plans, procedures, and test cases at all levels as outlined in the contractor TEMP. The contractor shall create and maintain a traceability of Phase requirements, including related interface requirements, to test cases. The contractor shall document the results of all testing.

The contractor shall test the readability and formatting of all migrated data in preparation for system level testing.

5.3.3 Task 3 Subtask 3-Phase Implementation and Integration

The contractor shall perform all activities necessary to execute system level functional, performance, interface, and integration testing of each Phase in factory, limited-deployment, and full-deployment (operational) environments.

The contractor shall perform all activities necessary to deploy each Phase, including the supporting hardware, software, and data, to the operational locations. These activities include, but are not limited to, packaging, shipping, delivery, installation, integration, configuration, and check-out.

The contractor shall perform all activities necessary to fully configure all capabilities for operations. This includes delivering and installing all the software, initializing configuration files, configuring all of the accounts, establishing the organizational infrastructure to support workflow, defining all communities of interest and roles to support access controls. For the records management application, the contractor will implement the FBI provided file plan with the selected COTS software product. For the migrated data, the vendor will populate the record folder components and the record components with the appropriate metadata. The RM metadata will assist Records Management Division (RMD) in the management of FBI records.

The contractor shall perform all activities (extract, translate and error correction, load) necessary to migrate legacy data needed for the operation of capabilities delivered in each Phase. The contractor shall verify that no data required was lost or corrupted during the migration process. The contractor shall perform error correction as part of the data migration task. In support of legacy system shutdown, the contractor shall perform all activities necessary to migrate all necessary legacy data.

The contractor shall support the acceptance and transition of each Phase to full operations. The contractor shall support user acceptance test activities at the first user implementation site. For cost estimating purposes, the contractor shall assume a level of support of not more than two full-time equivalent staff for 60 working days (standard 8 hour work day) at a Washington Metropolitan area location.

The contractor shall support Government testing as outlined in the FBI SENTINEL TEMP. In support of Government tests, the contractor support activities shall include but not be limited to, keeping the system under test operational, providing access to all requested documentation; operating the system; performing requested procedures; answering questions and showing system and software configuration details. The contractor shall also establish and remove test accounts as required (both general and privileged).

5.3.4 Task 3 Subtask 4-Operations and Maintenance Support

In support to ongoing operations and maintenance, the contractor shall prepare and deploy modifications, patches and updates based on Government approved change requests to keep the deployed system operational. As applicable, these modifications, patches and updates shall be rolled forward into the

ongoing Phase baseline. All change requests will be approved by the Technical Configuration Control Board (TCCB) and the Change Management Board (CMB).

The contractor shall utilize implementing processes as mutually agreed to by the Government and the contractor.

The contractor shall utilize its technical governance processes for all changes recommended to the deployed technical baseline.

The contractor shall draft and forward for approval an O&M Service Level Agreement that meets the intent of the Task 4 Tiers -1 through -4 level of O&M support.

5.3.5 Task 3 Control Gates and Program Reviews

The following control gates and program reviews (ref. FBI IT LCMD) are applicable to this activity:

- Preliminary Design Review/ in conjunction with the DCR (for each Phase)
- Critical Design Review (for each Phase)
- Gate 3 - Final Design Review (FDR) (for each Phase)
- Product Test Readiness Review/Site Test Readiness Review/Site Acceptance Review (for each Phase)
- Gate 4/5 - Deployment Readiness Review/System Test Readiness Review (for each Phase)
- Operational Readiness Review (for each Phase)
- Gate 6 - Operational Acceptance Review (for each Phase)
- Delivery Acceptance Review (DAR) (for each Phase)

5.3.6 Task 3 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.4 Task 4-IT Operations and Maintenance

As directed by the Government, the contractor shall perform operations and maintenance for each deployed Phase (primary, backup and training string when deployed) at the levels of performance specified in the Government approved SLA.

A ramping up period prior to the formal start of operations and maintenance shall be required. During this period the contractor shall identify and train the staff needed to operate and maintain the system in sufficient time for the staff to participate as required in the operational testing (operational test and security test and evaluation) of the system. Formal Operations and Maintenance periods begin with a successful exit from the Operational Readiness Review at each increment. The contractor must coordinate with the Transition Management Unit (TMU) in FBI's Information Technology Operations Division (ITOD) to acquire an Operational Readiness Review (ORR) at each completed Phase.

The FBI ITOD operates on a four-Tier operations support structure. Each Tier is defined below.

Tier-1 Support:

- **What:** Provides remote helpdesk support to the end user (customer) from a phone call to the Enterprise Operation Center (EOC) via 202-324-1500.

- **When:** On-site support is available 24x7x365 day a year.
- **How:** The FBI's automated call distribution software routes the call to the first available helpdesk technician for support. The technician opens a call ticket via the FBI's trouble ticketing software product (Peregrine Systems ServiceCenter™). If the helpdesk technician can resolve the issue then the call ticket is closed. If the helpdesk technician cannot resolve the issue then a problem ticket is created from the call ticket and assigned to a Tier-2, Tier-3 or Tier-4 support entity (assignment group) for resolution. The ticket automatically is displayed in the assignment group's problem queue.
- **Functions:** Taking the customers call, creating call ticket, generating problem ticket (if necessary), remote troubleshooting, answering questions, password administration (resets, unlocks, unsuspend), profile related issues, desktop software and OS related issues, resolving user specific issues (not network, server, system, application or database issues), checking Tier-1 problem queue for tickets and reassigning (routing) them to the appropriate Tier-2, Tier-3 or Tier-4 assignment groups.

Tier-2 Support:

- **What:** Provides touch labor (on-site) support to systems and desktops, remote server and network support, remote account administration.
- **When:** On-site support is available during normal business hours, on-call evenings and weekends. The EOC (SysAdmin/Network) is available on-site 24x7x365 days a year.
- **How:** Tier-2 support groups are responsible for checking their problem queues, acknowledging, assigning and updating ticket with status of troubleshooting. Once the issues are resolved, the Tier-2 Group is responsible for ensuring the integrity of the ticket, entering appropriate resolution, contacting the customer (when appropriate) and closing the ticket. When appropriate, the Tier-2 Group is responsible for preparing scripts or procedures to document corrective actions for lower tier support use.
- **Functions:** Monitoring of enterprise networks and system enclaves, monitoring of enterprise and system servers, remote network and server support, remote server and desktop virus updates, desktop hardware support, laptop support, network hardware support, account administration (new, modified or deleted account).

Tier-3 Support:

- **What:** Provides application, systems, network, server and mainframe support.
- **When:** On-site support is available during normal business hours, on-call evenings and weekends.
- **How:** Tier-3 support groups are responsible for checking their problem queues, aeknowledging, assigning and updating ticket with status of troubleshooting. Once the issues are resolved, the Tier-3 Group is responsible for ensuring the integrity of the ticket, entering appropriate resolution, contacting the customer (when appropriate) and closing the ticket. When appropriate, the Tier-3 Group is responsible for preparing scripts or procedures to document corrective actions for lower tier support use.
- **Functions:** OS patch management

Tier-4 Support:

- **What:** Provides support to systems ' databases, re-engineering or issues that occur outside of normal operations.
- **When:** On-site support is available during normal business hours, on-call evenings and weekends.
- **How:** Tier-4 support groups are responsible for checking their problem queues, acknowledging, assigning and updating ticket with status of troubleshooting. Once the issues are resolved, the Tier-4 Group is responsible for ensuring the integrity of the ticket, entering appropriate resolution, contacting the customer (when appropriate) and closing the ticket. When appropriate, the Tier-4 Group is responsible for preparing scripts or procedures to document corrective actions for lower tier support use.

- **Functions**: Re-engineering of current system, software licensing & maintenance support, resolving database errors or enhancements to current databases, testing enhancements to applications and baselines.

The contractor shall implement an operations and maintenance approach consistent with the Tier approach as defined above. The FBI's ITOD will perform Tier-1 activities. Coordinating jointly with the FBI's ITOD, the contractor shall be responsible for Tiers-2, -3 and -4 activities.

Definition of Normal Business Hours: 7:30 a.m. – 4:00 p.m. EST (Monday – Friday).

5.4.1 Task 4 Subtask 1-Pre-Full Operational Capability (FOC) Operations and Maintenance (separately priced options for O&M of each Phase)

Note: FOC occurs at the completion of the final incremental Phase (Phase 4) deployment

5.4.1.1 Conduct System Administrator Training

The contractor shall conduct training in accordance with the approved Training Plan. The contractor shall provide training for SENTINEL Phases prior to them being delivered. The contractor shall be responsible for the generation and distribution of all training materials.

5.4.1.2 Conduct of Pre-FOC Operations and Maintenance

Note that Tier-4 activities are addressed under Task 3 during Pre-FOC Operations and Maintenance.

The contractor shall conduct Tier-2 and Tier-3 operations and maintenance as required for each deployed Phase to ensure the service levels agreed to in the SLA are sustained and the system certification is maintained. Operations tasks include, but are not limited to:

- System administration including performance of authorized configuration changes (e.g., adding user accounts, changing passwords, modifying workflow groups) in accordance with the established procedures.
- Develop and maintain scripts and procedures in support of Tier-1, -2, -3, and -4 activities.
- Maintain an inventory of hardware and software on site and perform site configuration management. Equipment that is purchased for SENTINEL must be placed in the FBI's Property Management Application (PMA). Inventory of Hardware and Software shall be managed by the contractor.
- Maintain system security in accordance with the approved procedures. The hardware being proposed for SENTINEL must be capable of supporting the FBI's existing security policies.
- Make software changes/corrections as directed by the Government and in accordance with FBI CM procedures.
- Ensure all documentation is updated as changes are made in accordance with CM procedures.
- Interact closely with ITOD for purposes of knowledge transfer, roll changes into next release, etc.
- Conduct Hardware and Software License and Warranty Management including coordinating with FBI ITOD for warranty support for items covered under the FBI's enterprise warranties.
- Deploy and test patches, updates, and other modifications in accordance with approved Patch Management procedures (SUS Patch Management Roadmap and associated procedures).
- The contactor shall maintain the established configuration baseline and adhere to the established configuration management process.
- The contractor will need to provide CM resources for the following CM activities: Configuration Identification, Change Management, Configuration Status, Accounting, Audit, and Release

Management. These CM Activities are defined in the FBI CM Plan.

- Maintain the offline environments (e.g. development, test, staging, etc.) required to support operations and maintenance activities.
- Respond to and resolve problem tickets in the amount of time agreed to in the SLA.

Any actions or changes not explicitly authorized via the baselined O&M and accreditation documents shall be documented via a Change Request. The Government will approve all Change Requests. All proposed baseline changes shall be reviewed for impact to both the operational and development baseline. The Government will be the approving authority for all Change Requests utilizing the process defined in the FBI CM Plan.

5.4.2 Task 4 Snbtask 2-Operations and Maintenance Transition (separately priced option)

The Government may choose to transition Operations and Maintenance immediately following the FOC deployment or at any time during the two years following the FOC deployment. In the event that not all Phase options are exercised, the Government may initiate the transition task in conjunction with or following the last exercised Phase option.

5.4.2.1 Condnct System Administrator Training

The contractor shall conduct training in accordance with the approved Training Plan. The contractor shall provide training for SENTINEL Phases prior to them being delivered. The contractor shall be responsible for the generation and distribution of all training materials.

5.4.2.2 Condnct Operations and Maintcnance

Upon request, the contractor shall implement and ensure a seamless transition of Tiers -2, -3 and -4 operations and maintenance activities to thc FBI ITOD within a 6-month period. The transition task shall include but is not limited to:

- Classroom and on the job training of system administrators and privileged users.
- Collaborative conduct of operations and maintenance during the transition period.
- Identify number of resources and skill set required by the FBI to assume O&M responsibilities.
- Develop Roles and Responsibilities for the different ITOD entities for O&M functions.
- The contractor shall hold briefings to educate the FBI about trace O&M entitlement, subcontracting accomplishments, and all related requirements that were developed on behalf of the FBI.
- Transition all hardware, software, and licenses to the FBI (ITOD). All warranty and maintenance terms need to be documented and provided to the FBI.
- Ensure that all System documentation is current.
- Development of an O&M transition plan as defined in the list of Deliverables.

During the dcsignated transition period, the contractor shall be responsible for the established SLAs.

5.4.3 Task 4 Subtask 3 Post-FOC Operations and Maintenance and Sustainment (separately priced options for two one-year periods)

5.4.3.1 Conduct System Administrator Training

The contractor shall conduct training in accordance with the approved Training Plan. The contractor shall provide training for SENTINEL Phases prior to them being delivered. The contractor shall be responsible for the generation and distribution of all training materials.

5.4.3.2 Conduct Operations and Maintenance

The contractor shall conduct operations and maintenance (Tier-2, -3, and -4) for the FOC system ensuring the service levels agreed to in the SLA are maintained and the system certification is maintained. Tasks include, but are not limited to:

- Planning for and implementation of a technology refreshment program.
- System administration including performance of authorized configuration changes (e.g., adding user accounts, changing passwords, modifying workflow groups) in accordance with the established procedures.
- Develop and maintain scripts and procedures in support of Tier-1, -2, -3, and -4 activities.
- Maintain an inventory of hardware and software on site and perform site configuration management. Equipment that is purchased for SENTINEL must be placed in the FBI's Property Management Application (PMA). Hardware and software inventory shall be managed by the contractor.
- Maintain system security in accordance with the approved procedures.
- Make software changes/corrections as directed by the Government and in accordance with FBI CM procedures. Note that post FOC, all Tier 4 activities are conducted under Task 4.
- Ensure all documentation is updated as changes are made in accordance with CM procedures.
- Conduct Hardware and Software License and Warranty Management.
- Deploy and test patches, updates, and other modifications in accordance with approved Patch Management procedures. Refer to Section 15 for details.
- The contactor shall maintain the established configuration baseline and adhere to the established configuration management process.
- The contractor will need to provide CM resources for the following CM activities: Configuration Identification, Change Management, Configuration Status, Accounting, Audit, and Release Management. These activities are defined in the FBI SENTINEL CM Plan
- Respond to and resolve problem tickets in the amount of time agreed to in the SLA.

Any actions or changes not explicitly authorized via the baselined O&M and accreditation documents shall be documented via a Change Request. The Government will approve all Change Requests. All proposed baseline changes shall be reviewed for impact to the operational baseline. The Government will be the approving authority for all Change Requests utilizing pre-defined boards.

5.4.4 Task 4 Control Gates and Program Reviews

The following control gates and project reviews (ref. FBI IT LCMD) are applicable to this activity:

- Annual Operations Review

5.4.5 Task 4 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

5.5 Task 5-Organizational Change Management

As SENTINEL services are deployed, the FBI will dramatically change its way of doing business. To ensure a smooth transition and full adoption by the SENTINEL customer base, an organizational change management program is needed.

The contractor shall perform all activities necessary to develop and implement an effective Organizational Change Management program. The contractor shall market, develop training materials, conduct training and provide continued user support as required to ensure full adoption of SENTINEL and its associated business processes. All user contact shall be conducted in coordination with the Government program office.

5.5.1 Task 5 Subtask 1-Assess and Plan Change Management

The contractor shall work collaboratively with FBI personnel to analyze and develop the SENTINEL Stakeholder and Organizational Risk Assessment (SSORA). This information shall be a critical input to Workforce Transformation (WFT) activities during subsequent SENTINEL deployments. This document shall provide input to workforce transition plans and activities required for successful transition to new roles and responsibilities of end users, the communication and stakeholder management plan, and the development of a training plan.

The SSORA will serve as a guide for detailed planning and execution of all SENTINEL change management activities.

The contractor shall analyze and generate an Organization Impact Assessment (OIA) to identify organization-wide impacts of SENTINEL on FBI law enforcement processes and/or systems. The contractor shall follow the SENTINEL Risk Management process to document any risks identified in the OIA.

The contractor shall develop a Workforce Transformation Strategy and Plan based on the SSORA and OIA.

5.5.2 Task 5 Subtask 2-Develop Training Material

5.5.2.1 Training Strategy and Plan

The contractor shall develop and implement a detailed SENTINEL Training Strategy and Plan for FBI users that relates SENTINEL processes by Phases to deployment schedules. The plan shall identify how to leverage and seamlessly integrate Technology Based Training (TBT) (e.g., Web-based, computer based training, distance learning) and instructor lead training across each SENTINEL Phase while managing effects on FBI law enforcement operations; identify SENTINEL user group profiles by geographic location; analyze SENTINEL training for impacts on the FBI workforce, and analyze training to accommodate steep learning curves and changes in work roles and responsibilities. The plan shall coordinate training activities with FBI wide training initiatives. The plan shall include a knowledge transfer and integration strategy for the transference of SENTINEL training to the FBI Training Academy and Field Office training teams.

The contractor shall propose a suitable user training package to accommodate both new and existing employees. Such a package may include TBTs, a user's manual and/or any other such materials identified in the approved Training Strategy and Plan.

The contractor shall analyze and report on the FBI's existing training administration processes to determine how training participation is recorded. If necessary, the contractor shall recommend a reproducible SENTINEL training administration solution, and implement the FBI approved solution for recording and tracking participation in SENTINEL training.

5.5.2.2 Training Media

Training media may include TBT, instructor-lead, user manuals (automated and written), Frequently Asked Questions (FAQs), in addition to the "context-sensitive" help embedded in the application. TBT shall be delivered from a SENTINEL website that is seamlessly integrated into the SENTINEL application. In cases where instructor-lead training is beneficial, the contractor shall arrange for an appropriately equipped facility (if the Government is unable to provide same) and trainers. Training instructors shall be certified (e.g., Amercian Society for Training and Development, FBI Academy)

5.5.2.3 Technology-Based Training

The contractor shall exploit modern TBT wherever possible and shall deliver these packages in a manner and form eompatible with the SENTINEL system. The contractor shall follow the Sharable Content Objeet Reference Model (SCORM) which aims to foster creation of reusable learning content as "instructional objects" within a common technieal framework for computer and technology-based learning. The contraetor shall arrange for an appropriately equipped facility (if the Government is unable to provide the same).

5.5.3 Task 5 Subtask 3-Conduct User Training

The contractor shall conduct training in accordance with the FBI approved Training Strategy and Plan. The contraetor shall provide training for SENTINEL serviees as they are delivered. Training will begin upon receipt of Authority to Operate; however, for the first implementation site (see paragraph 5.3.3) training must be completed immediately before the receipt of Approval to Operate. The contractor shall be responsible for the generation and distribution of all training materials.

Training shall be accomplished in a decentralized fashion at each of the FBI Field Offices and foreign Legal Attaché posts. Training shall also be accomplished at Resident Agencies with 50([TBR- *Offeror to update as appropriate based on proposed training approach*) or more field agents attached to the location.

The contractor shall develop and perform a repeatable process for analyzing and resolving user identified training problems, feedback, and lessons learned and communicate the results to the FBI Communications and performance engineering teams. The results will include a matrix categorizing the training problems. The matrix shall include the severity, frequency, and resolution plans for the problem, identifying how the curriculum will be reetified.

5.5.4 Task 5 Subtask 5-Continued User Support

The eontractor shall provide user assistance (facilitators) at the selected training locations (see paragraph 5.3.3) for two weeks (target, location dependent) following the training. Travel to smaller offices may be required.

5.5.5 Task 5 Subtask 6-Extended Support

The contractor shall provide the following extended support to the new process activities: incorporation of paper-only documents, incorporation of photos, individual tutoring of field personnel, and incorporation of historical information related to open cases that have migrated to SENTINEL. For estimating purposes assume this support begins with the completion of Task 5 Subtask 5 and continues for an additional 2 weeks at each location where training is provided. Travel to smaller offices may be required.

5.5.6 Task 5 Subtask 7-Support to Government Communications

The contractor shall develop and execute a Communications Plan (CP) for audiences having interest in SENTINEL in order to promote their understanding of the benefits of SENTINEL. The CP shall describe messages tailored to each audience's perspectives and shall state how these messages will be delivered in a

timely manner through channels and in formats most relevant to each audience. Audiences of interest include: FBI employees who are not expected to be users of SENTINEL; oversight agencies and Congress; government agencies not expected to participate; the media; and groups interested in the technical and program management aspects of SENTINEL.

The contractor shall create comprehensive messages and supporting documentation, which clearly explain the mission, vision, and goals of the SENTINEL program. The contractor shall support communications activities that create awareness and understanding of the SENTINEL initiative, approaches, values, and general deployment timeframes. The contractor shall produce communications content and products that address the unique needs and roles of various audiences. The contractor shall craft communications messages containing baseline SENTINEL program information including, but not limited to, schedule, milestones, functionality descriptions, and benefits. The contractor shall conduct analyses and assessments of communications activities based on research, feedback, and lessons learned. The contractor shall use this information to develop ways to improve its communications planning, activities, and performance.

The contractor shall develop content for FBI communications products including briefings, interview talking points, presentations, internal FBI newsletters, FBI Management Toolkits, frequently asked questions (FAQs) requests, fact sheets, FBI Web portal content, Congressional questions for the record (QFRs), reports to Congress, and other media, as requested.

The contractor shall develop specific demonstrations as a communications tool (not a training tool) with accompanying User Guide of the features of SENTINEL. The demonstrations may be developed for both internal (FBI) and external stakeholders for each Phase.

5.5.7 Task 5 Control Gates and Program Reviews

The following control gates and project reviews (ref. FBI IT LCMD) are applicable to this activity:

- Requirements Clarification Review (2 weeks after CIR for Phase 1, in conjunction with CIR for Phases 2-4)
- Design Concept Review (in conjunction with Phase PDR)
- Preliminary Design Review/ in conjunction with the Design Concept Review (for each Phase)
- Critical Design Review (for each Phase)
- Gate 3 - Final Design Review (FDR) (for each Phase)
- Product Test Readiness Review/Site Test Readiness Review/Site Acceptance Review (for each Phase)
- Gate 4/5 - Deployment Readiness Review/System Test Readiness Review (for each Phase)
- Operational Readiness Review (for each Phase)
- Gate 6 - Operational Acceptance Review (for each Phase)
- Annual Operational Review (yearly after first delivery)
- Delivery Acceptance Review (DAR) (for each Phase)

5.5.8 Task 5 Deliverables

A listing of data items applicable to this task is provided in SOW paragraph 9.1.

6. Contract Type

Development and Organizational Change Management (Contract Line Item Numbers) CLINs will be awarded on a cost plus award fee basis using the performance-based SOW requirements as the basis for performance.

Material CLINs will be awarded on a cost reimbursement with fixed material handling fee. The Government reserves the right to substitute GFE for all proposed items in the material CLIN.

Travel CLINs will be awarded on a cost reimbursement basis.

Operations and Maintenance CLINs will be awarded on a cost plus award fee basis using Service Level Agreements when applicable.

7. Place of Performance

Although some work will be accomplished at FBI facilities, the primary site for work associated with this Task Order shall be the contractor's facility. Program management, systems engineering, design, development, integration and initial system level testing will be performed at the contractor's facility. Elements of implementation and integration including final system and enterprise integration testing, organizational change management, and operations and maintenance will be performed at Government facilities. The Clarksburg, WV. Data Center will serve as the primary site and the Washington D.C. Data Center as the backup and site test location. Other locations will be made available as required and requested.

8. Period of Performance

The base period of performance for Phase 1 development is nominally 12 months. Successful completion of Phase 1 is at Delivery Acceptance Review. SENTINEL's subsequent option periods are to follow a similar period of performance. Period of performance is TBS. *[Tto be proposed as part of proposal.]* The Government will provide a 30-day notice of intent before each option is to be exercised.

9. Deliverables/Delivery Schedule

9.1 Data Requirements

Table 9.1-1 contains a listing of data requirements by SOW Task. The complete delivery schedule tied to FBI IT LCMD Program Reviews is contained in Attachment-3. The Attachment 3 delivery schedule deviates from the suggested schedule contained in the FBI IT LCMD to accommodate the tailoring of the Control Gates and Program Reviews. Documents required for a given review or control gate shall be delivered as soon they are available and must be delivered no later than one week prior to the review or control gate. Delivery requirements for non-gate/review items are in Table 9.I-1 below and in the Section 18 descriptions.

Descriptions of data items can be found in the FBI IT LCMD Appendix H, the FBI C&A Handbook, and in Section 18 of the SOW. Where there are descriptions provided in both the FBI IT LCMD and in the SOW, the description in the SOW shall prevail.

The referenced Data Item Descriptions are for functional guidance as to the technical content.

Distribution of the required data is limited to authorized United States Government Agencies only.

Any contractor-imposed distribution restrictions shall be noted on the cover page, all applicable pages, and

all specific paragraphs that contain information with contractor-imposed restricted distribution requirements.

Copies of the Data Items shall be delivered in both hard copy and electronic format. Hectronic format shall be in one of the following formats as applicable to the type of data delivered: Microsoft Word 2000, Microsoft PowerPoint 2000, Microsoft Excel 2000, or specific format approved by the Contracting Officer's Technical Representative (COTR).

Electronic formatted data items shall be delivered on CD-ROM disks and labeled with the document title, document number assigned by the COTR (if any), version/revision number (if any), security classification, **file type, "Preliminary," "Draft," "Final," or "Baseline" annotation, Data Item number, document date, copy information, and special handling instructions (if auy). Electrouic formatted data shall be virus scanned and free from any known virus iu compliance with FBI security requirements.**

All data items shall be delivered electronically on CD-ROM disks to the Program Manager (PM) and in hardcopy to the PM, Contracting Officer's Technical Representative (COTR), and the Contracting Officer (CO).

Unless otherwise noted, the comment and update period is three wecks for each document: two weeks for Government review and one week for the contractor to complete the update.

All data items require Government approval unless otherwise noted.

Procedures included or referenced in the data items shall be written at the keystroke level. This guidance applies to data items including, but not limited to, the Privileged User Security Guide, General User Security Guide, System Operations and Maintenance Manual, Users Manual, and the Software Installation Manual.

Commercial hardware and software manuals shall be delivered and are suitable substitutes for the technical manual deliverables. Technical manuals are only required in the event a commercial manual is not available, off-the-shelf hardware or software is modified, or custom hardware or software is developed. Commercial manuals in conjunction with addenda are also acceptable when appropriate.

Table 9.1-1 Task Order Data Requirements

Data Item Number	Document Title	Applicable Task	Description Source
0076	Agendas, Briefings, Meeting Minutes (as required)	5.0 (all)	SOW Section 18
0073	Analysis/Trade Study Report (as required)	5.0 (all)	FBI IT LCMD App H
0015	Bill of Materials	5.1.2	FBI IT LCMD App H
0016	Configuration Management Plan	5.1.2	FBI IT LCMD App H
0004	Contract Funds Status Report (CFSR) (monthly)	5.1.2	SOW Section 18
0007	Defect Reports (monthly with Measurement Report)	5.1.2	SOW Section 18
0005	Earned Value Mgmt. Sys. (EVMS) Report (Monthly)	5.1.2	SOW Section 18
0012	EOC Memorandum of Understanding	5.1.2	SOW Section 18
0078	Integrated Master Plan	5.1.2	SOW Section 18
0014	Integrated Master Schedule (weekly)	5.1.2	SOW Section 18
0008	Measurement Plan (incl CPMs)	5.1.2	SOW Section 18
0009	Measurement Report (monthly)	5.1.2	SOW Section 18
0017	Quality Assurance Plan	5.1.2	FBI IT LCMD App H

0013	Risk Assessment (delivered twice monthly)	5.1.2	SOW Section 18
0006	Risk Management Plan	5.1.2	SOW Section 18
0003	Security Plan	5.1.2	FBI IT LCMD App H
0001	Task Order Management Plan	5.1.2	SOW Section 18
0011	Travel Plan (update quarterly)	5.1.2	SOW Section 18
0050	Version Description Document	5.1.2	FBI IT LCMD App H
0018	Data Accession List	5.1.3	SOW Section 18
0002	In Progress Review Report (monthly)	5.1.4	SOW Section 18
0034	Certification Test Plan	5.2.1	FBI C&A Handbook
0039	Data Migration Plan	5.2.1	SOW Section 18
0022	Operations and Maintenance Design Document	5.2.1	FBI IT LCMD App H
0026	Requirements Clarification Document	5.2.1	FBI IT LCMD App H
0074	Requirements Traceability Matrix	5.2.1	FBI IT LCMD App H
0030	Security Implementation Plan	5.2.1	FBI C&A Handbook
0023	System Design Document	5.2.1	FBI IT LCMD App H
0020	System Specification	5.2.1	FBI IT LCMD App H
0024	Systems Engineering Management Plan	5.2.1	FBI IT LCMD App H
0037	Test and Evaluation Master Plan	5.2.1	FBI IT LCMD App H
0047	Training Plan	5.2.1	FBI IT LCMD App H
0021	Transition Plan	5.2.1	FBI IT LCMD App H
0025	Design Concept Description and Architecture	5.2.2	SOW Section 18
0066	Logical Data Model	5.2.2	SOW Section 18
0058	Software Development Plan	5.3.0	FBI IT LCMD App H
0081	Delivery Acceptance Report	5.3.0, 5.5	SOW Section 18 TBS
0059	Database Design Document (DBDD)	5.3.1	FBI IT LCMD App H
0044	Interface Control Document	5.3.1	FBI IT LCMD App H
0045	Interface Design Document	5.3.1	FBI IT LCMD App H
0054	Systems Operations and Maintenance Manual	5.3.1	FBI IT LCMD App H
0053	Technical Manual (Non-Commercial HW only)	5.3.1	SOW Section 18
0031	General User Security Guide	5.3.2	FBI C&A Handbook
0032	Privileged User Security Guide	5.3.2	FBI C&A Handbook
0051	Software Installation Manual	5.3.2	FBI IT LCMD App H
0049	Software Product Specification	5.3.2	FBI IT LCMD App H
0028	System Security Plan	5.3.2	FBI C&A Handbook
0048	Test Procedures	5.3.2, 5.3.3	FBI IT LCMD App H
0052	Test Report	5.3.2, 5.3.3	FBI IT LCMD App H
0055	Training Materials	5.3.2, 5.5.2	FBI IT LCMD App H
0029	Certification Test Plan (ST&E) (Development)	5.3.3	FBI C&A Handbook
0041	DCU04 Request for Data Center Access	5.3.3	SOW Section 18
0042	DCU05 Request for Data Center Equipment Installation	5.3.3	SOW Section 18
0061	Installation Drawings	5.3.3	FBI IT LCMD App H

0046	Installation Plan	5.3.3	FBI IT LCMD App H
0065	Product (CSCI's)	5.3.3	SOW Section 18
0027	Contingency Plan	5.3.3	FBI C&A Handbook
0040	EOC Operational Support Requirements Document of New Systems	5.3.4	SOW Section 18
0036	Service Level Agreement	5.3.4	SOW Section 18
0068	O&M Procedures	5.3.4, 5.4	SOW Section 18
0057	Operational Readiness Report	5.3.5	FBI IT LCMD App H
0069	O&M Transition Plan	5.4.2	SOW Section 18
0071	Organization Impact Assessment	5.5.1	SOW Section 18
0070	SENTINEL Stakeholder and Organizational Risk Assessment (SSORA)	5.5.1	SOW Section 18
0077	Workforce Transformation Strategy and Plan	5.5.1	SOW Section 18
0080	Training Administration Report	5.5.2	SOW Section 18
0079	Training Strategy and Plan	5.5.2	SOW Section 18
0072	User Manual	5.5.2	FBI IT LCMD App H
0010	Communications Plan	5.5.6	SOW Section 18

9.2 Task Order Delivery Schedule (TBR)

Table 9.2-1 contains the CLIN structure and delivery schedule for the task order including the priced options.

INSTRUCTION:
As part of the proposal the contractor shall fill in the proposed durations and start and end dates in Table 9.2-1.

Table 9.2-1 Delivery Schedule

CLIN #	CLIN/SUB CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months)	Start Date (Calendar months after contract award)	Finish Date (Calendar months after contract award)	Contract Type	Notional Earned Value Type
				TBS	TBS	TBS		
1	**Phase 1 Development and Deployment**	**Base**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
1.1	Phase 1 Program Management	Base	5.1				CPAF	Deliverables & LOE
1.2	Phase 1 Systems Engineering and Architecture	Base	5.2				CPAF	Deliverables & LOE
1.3	Phase 1 Design, Development, Integration,	Base	5.3				CPAF	Deliverables & LOE

CLIN #	CLIN/SUB CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months) TBS	Start Date (Calendar months after contract award) TBS	Finish Date (Calendar months after contract award) TBS	Con-tract Type	Notional Earned Value Type
	Deployment, and Testing							
2	**Phase 2 Development and Deployment**	**Option**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
2.1	Phase 2 Program Management	Option	5.1				CPAF	Deliverables & LOE
2.2	Phase 2 Systems Engineering and Architecture	Option	5.2				CPAF	Deliverables & LOE
2.3	Phase 2 Design, Development, Integration, Deployment, and Testing	Option	5.3				CPAF	Deliverables & LOE
3	**Phase 3 Development and Deployment**	**Option**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
3.1	Phase 3 Program Management	Option	5.1				CPAF	Deliverables & LOE
3.2	Phase 3 Systems Engineering and Architecture	Option	5.2				CPAF	Deliverables & LOE
3.3	Phase 3 Design, Development, Integration, Deployment, and Testing	Option	5.3				CPAF	Deliverables & LOE
4	**Phase 4 Development and Deployment**	**Option**	**5.1, 5.2, 5.3**				**CPAF**	**Deliverables & LOE**
4.1	Phase 4 Program Management	Option	5.1				CPAF	Deliverables & LOE
4.2	Phase 4 Systems Engineering and Architecture	Option	5.2				CPAF	Deliverables & LOE
4.3	Phase 4 Design, Development, Integration, Deployment, and Testing	Option	5.3				CPAF	Deliverables & LOE
5	**Organizational Change Management**	**Both**	**5.1, 5.5**				**CPAF**	**Deliverables & LOE**
5.1	Phase 1 Organizational Change Management	Base	5.1, 5.5				CPAF	Deliverables & LOE
5.2	Phase 2 Organizational Change Management	Option	5.I, 5.5				CPAF	Deliverables & LOE
5.3	Phase 3 Organizational Change Management	Option	5.1, 5.5				CPAF	Deliverables & LOE
5.4	Phase 4 Organizational Change Management	Option	5.1, 5.5				CPAF	Deliverables & LOE

CLIN	CLIN/SUB CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months)	Start Date (Calendar months after contract award)	Finish Date (Calendar months after contract award)	Contract Type	Notional Earned Value Type
				TBS	TBS	TBS		
6	**Operations and Maintenance**	**Option**	**5.1, 5.4**				**CPAF SLA Based**	**Deliverables**
6.1	Phase 1 (pre-FOC) Operations and Maintenance	Option	5.1, 5.4				CPAF SLA Based	LOE
6.2	Phase 2 (pre-FOC) Operations and Maintenance	Option	5.1, 5.4				CPAF SLA Based	LOE
6.3	Phase 3 (pre-FOC) Operations and Maintenance	Option	5.1, 5.4				CPAF SLA Based	LOE
6.4	Year 1 Post FOC Operations and Maintenance	Option	5.1, 5.4	12			CPAF SLA Based	LOE
6.5	Year 2 Post FOC Operations and Maintenance	Option	5.1, 5.4	12			CPAF SLA Based	LOE
6.6	Operations and Maintenance Transition	Option	5.1, 5.4	6			CPAF	LOE
7	**Materials (Hardware and Software)**	**Both**	**5.1, 5.2, 5.3, 5.4, 5.5**				**CPFF**	**Deliverables**
7.1	Phase 1 Development and Deployment Materials	Base	5.1, 5.2, 5.3				CPFF	Deliverables
7.2	Phase 2 Development and Deployment Materials	Option	5.1, 5.2, 5.3				CPFF	Deliverables
7.3	Phase 3 Development and Deployment Materials	Option	5.1, 5.2, 5.3				CPFF	Deliverables
7.4	Phase 4 Development and Deployment Materials	Option	5.1, 5.2, 5.3				CPFF	Deliverables
7.5	Phase 1 (pre-FOC) Operations and Maintenance Materials	Option	5.1, 5.4				CPFF	Deliverables
7.6	Phase 2 (pre-FOC) Operations and Maintenance Materials	Option	5.1, 5.4				CPFF	Deliverables
7.7	Phase 3 (pre-FOC) Operations and Maintenance Materials	Option	5.1, 5.4				CPFF	Deliverables
7.8	Year 1 Post FOC Operations and Maintenance Materials	Option	5.1, 5.4	12			CPFF	Deliverables
7.9	Year 2 Post FOC Operations and Maintenance Materials	Option	5.1, 5.4	12			CPFF	Deliverables

CLIN	CLIN/SUB CLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months) TBS	Start Date (Calendar months after contract award) TBS	Finish Date (Calendar months after contract award) TBS	Con-tract Type	Notional Earned Value Type
7.10	Operations and Maintenance Transition Materials	Option	5.1, 5.4	6			CPFF	Deliverables
7.11	Phase 1 Organizational Change Management Materials	Base	5.1, 5.5				CPFF	Deliverables
7.12	Phase 2 Organizational Change Management Materials	Option	5.1, 5.5				CPFF	Deliverables
7.13	Phase 3 Organizational Change Management Materials	Option	5.1, 5.5				CPFF	Deliverables
7.14	Phase 4 Organizational Change Management Materials	Option	5.1, 5.5				CPFF	Deliverables
8	**Travel**	**Both**	**5.1, 5.2, 5.3, 5.4, 5.5**				**CR**	**Deliverables**
8.1	Phase 1 Development and Deployment Travel	Base	5.1, 5.2, 5.3				CR	Deliverables
8.2	Phase 2 Development and Deployment Travel	Option	5.1, 5.2, 5.3				CR	Deliverables
8.3	Phase 3 Development and Deployment Travel	Option	5.1, 5.2, 5.3				CR	Deliverables
8.4	Phase 4 Development and Deployment Travel	Option	5.1, 5.2, 5.3				CR	Deliverables
8.5	Phase 1 (pre-FOC) Operations and Maintenance Travel	Option	5.1, 5.4				CR	Deliverables
8.6	Phase 2 (pre-FOC) Operations and Maintenance Travel	Option	5.1, 5.4				CR	Deliverables
8.7	Phase 3 (pre-FOC) Operations and Maintenance Travel	Option	5.1, 5.4				CR	Deliverables
8.8	Year 1 Post FOC Operations and Maintenance Travel	Option	5.1, 5.4	12			CR	Deliverables
8.9	Year 2 Post FOC Operations and Maintenance Travel	Option	5.1, 5.4	12			CR	Deliverables
8.10	Operations and Maintenance Transition Travel	Option	5.1, 5.4	6			CR	Deliverables
8.11	Phase 1 Organizational Change Management Travel	Base	5.1, 5.5				CR	Deliverables
8.12	Phase 2 Organizational Change Management Travel	Option	5.1, 5.5				CR	Deliverables

CLIN #	CLIN/SUBCLIN Name	Base Contract and/or Contract Option	Applicable TORP Task Number(s)	Duration (Calendar months) TBS	Start Date (Calendar months after contract award) TBS	Finish Date (Calendar months after contract award) TBS	Contract Type	Notional Earned Value Type
8.13	Phase 3 Organizational Change Management Travel	Option	5.1, 5.5				CR	Deliverables
8.14	Phase 4 Organizational Change Management Travel	Option	5.1, 5.5				CR	Deliverables
9	**GWAC Fees to NIH**	**Both**	**5.1, 5.2, 5.3, 5.4, 5.5**				**GWAC FEE**	**LOE**
9.1	FY 06 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.2	FY 07 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.3	FY 08 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.4	FY 09 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.5	FY 10 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE
9.6	FY 11 GWAC Fees to NIH	Both	5.1, 5.2, 5.3, 5.4, 5.5				GWAC FEE	LOE

10. Security

10.1 Personnel and Facility Clearance Requirements

The contractor shall abide by the requirements set forth in the Contract Security Classification Specification (DD Form 254).

The contractor shall develop and maintain a comprehensive security program to address the security needs of the SENTINEL program.

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual shall interface with the FBI Security Office on all security matters, to include physical, personnel and protection of all Government information and data accessed by the contractor.

10.1.1 Personnel Requirements

Personnel clearance requirements are contained in the attached DD Form 254. Contractors who will have access to FBI facilities, systems or data shall possess an active and transferable Top Secret clearance at the time of proposal submission. The Government reserves the right to waive this requirement for any portion of the work that deals with technologies or data that is in the public domain.

10.1.2 Facility Security Requirements

Facility security requirements are contained in the attached DD Form 254.

10.2 Security Acquisition Section Requirements

10.2.1 Access to Classified Information

Notwithstanding the provisions of Section 3 of the NISPOM, the Government intends to secure services or equipment from firms that are not under foreign ownership, control or influence (FOCI) or where any FOCI, in the opinion of the Government, adversely impacts on security requirements. The Government reserves the right to contract with such Offerors under appropriate arrangements, when it determines that such contract will be in the best interest of the Government.

Accordingly, all Offerors responding to this proposal or initiating performance of a contract are required to submit a Certificate Pertaining to Foreign Interests (SF 328) or update a previously submitted SF 328, and a Key Management Personnel List (KMPL) with their proposal. All SF 328s and KMPLs shall be executed at the parent and subsidiary levels of an organization. Offerors are also required to request, collect, and forward to the Government the SF 328 from all subcontractors undertaking classified work under the Offeror's direction and control. Offerors are responsible for the thoroughness and completeness of each subcontractor's SF 328 submission. SF 328 entries should specify, where necessary, the identity, nature, degree, and impact of any FOCI on their organization or activities, or the organization or activities of a subcontractor. Additionally, a KMPL must be submitted with each SF 328 which identifies senior management by name, position, social security number, date/place of birth, and citizenship status.

The Offeror shall, in any case in which it believes that foreign influence exists or is being sought over its affairs, or the affairs of any subcontractor, promptly notify the Contracting Officer's Security Representative of all pertinent facts, even if such influence is not exerted to the degree specified in the NISPOM.

The Offeror shall provide an updated SF 328 and KMPL no later than five years from the date as certified on the last submitted SF 328. The contractor shall also promptly disclose to the Contracting Officer's Security Representative any information pertaining to any interest of a FOCI nature in the contractor or subcontractor that has developed at any time during the contractor's duration or has subsequently come to the contraetor's attention. An updated SF 328 is required of the contractor or any subcontractor whenever there is a change in response to any of the 10 questions on the SF 328.

The Offeror is responsible for initiating the submission of the SF 328 and KMPL for all subcontractors undertaking classified work during the entire period of performance of the contract. Failure to comply shall be cause for default under the Default Clause of this contract.

Offerors shall complete the Certificate Pertaining to Foreign Interests (SF 328) and Key Management Personnel Listing (KMPL) for the prime contractor and all proposed subcontractors. Submission should include identification of the proposal number, name of the assigned Contracting Officer and certification of the accuracy of the provided information by an Executive Management Official of the company. Provision of false information shall be cause for default under the Default Clause of this contract.

The Government reserves the right to prohibit individuals who are not U.S. citizens from all or certain aspects of the work to be performed under this contract. The Department of Justice (DOJ)/FBI does not permit the use of non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ IT system. By signing the contract or commitment document, the contractor agrees to this restriction.

Foreign Ownership, Control or Influence (FOCI) - For purposes of this elause, a U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company.

Changed conditions, such as change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating, or, alternatively, that a different FOCI mitigation measures be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI. **There is a continuing obligation of the selected Offeror to advise the Government of such changed conditions.** Failure to abide by this obligation shall be cause for default under the Default Clause of this contract.

Factors: The following factors will be used as the basis for making a FOCI determination. If the Offeror, or its proposed subcontractors, meet any of the following factors, they must identify themselves as a potential FOCI company and submit themselves to a Government FOCI evaluation and risk assessment:

(1) Ownership or beneficial ownership, direct or indirect, of 5 percent or more of the Offeror's company's voting securities by a foreign person.

(2) Ownership or beneficial ownership, direct or indirect, of 25 percent or more of any class of the Offeror's company's non-voting securities by a foreign person.

(3) Management positions, such as directors, officers or executive personnel of the Offeror's company held by non U.S. citizens.

(4) Foreign person power, direct or indirect, to control the election, appointment, or tenure of directors, officers or executive personnel of the Offeror's company or other decisions or activities of the Offeror's company.

(5) Contracts, agreements, understandings or arrangements between the Offeror's company and a foreign person.

(6) Loan arrangements between the Offeror's company and a foreign person if the Offeror's company's (the borrower) overall debt to equity ratio is 40:60 or greater; or financial obligations that are subject to the ability of a foreign person to demand repayment.

(7) Annual total revenues or net income in excess of 5 percent from a single foreign person or in excess of 30 percent from foreign persons in the aggregate.

(8) Ten percent or more of any class of the Offeror's voting securities held in "nominee shares", in "street names", or in some other method that does not disclose the beneficial ownership of equitable title.

(9) Interlocking directors with foreign persons and any officer or management official of the applicant company who is also employed by a foreign person;

(10) Any other factor that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of the Offeror's company.

(11) Ownership of 10 percent or more of any foreign interest.

Every effort must be made to ensure that supplies are provided and integrated and services are performed using sound security components, practices, and procedures. Acquisition of supplies or services from concerns under Foreign Ownership, Control or Influence (FOCI) or of supplies developed, manufactured, maintained or modified by concerns under FOCI (any or all of which shall be referred to herein as "Use of FOCI source") is of serious concern and must be approved prior to contract award and evaluated during contract performance. Approval decisions will be made on a case-by-case basis after the source or technology has been identified by the Offeror and subjected to a risk assessment.

The risk assessment process will vary depending on the acquisition type and proposed use of a FOCI source, available risk mitigation measures and the information/justification provided by the Offeror/contractor.

Any Offeror responding to this Request for Proposal (RFP), Request for Quotation (RFQ) or Sealed Bid acknowledges the Government's requirements to secure services or equipment from firms which are not under Foreign Ownership, Control or Influence (FOCI), or where any FOCI, in the opinion of the Government, adversely impacts on National Security or security requirements. The Offeror understands and agrees that the Government retains the right to reject any response to this RFP, RFQ or Sealed Bid made by the Offeror, without any further recourse by or explanation to the Offeror, if the FOCI for that Offeror is determined by the Government to be an unacceptable security risk.

Risk assessments will be on a case-by-case basis and will be used to determine whether the use of a FOCI source poses an unacceptable security risk. If an unacceptable security risk is determined, the Government retains the right to reject the use of a FOCI source or to require that certain risk mitigation measures be taken by the contractor. Similarly, the Government retains the unilateral right to approve the use of a FOCI source when the risk assessment indicates that such use would be in the Governments' best interests. If the use of a FOCI source is not approved, no classified information will be disclosed to the Offeror as part of the Government's rationale for non-approval. The Offeror (prime and subs) may not seek reimbursement from the Government for any costs associated with responding to this RFP, RFQ or Sealed Bid, as a result of a FOCI non-approval decision.

10.2.2 Products that Provide or Include Software and/or Hardware

As used in this clause, foreign-origin software and/or firmware is any software and/or firmware that is manufactured, developed, maintained and/or modified (1) outside the United States or its territories, or (2) in the United States or its territories by an individual who is not a citizen of the United States or its territories. Any degree of manufacture, development, maintenance or modification that meets either criterion (1) or (2) shall be sufficient for the software and/or firmware to be deemed foreign-origin under this clause.

The Government shall have the right to reject the offer of foreign-origin software and/or firmware during the solicitation or the supply of such software and/or firmware under the contract on a case-by-case basis. If the Government rejects the supply of foreign-origin software and/or firmware, the Government shall have the right to require a technically equal, or better, approved substitute or to terminate this contract for default. In the event that the software and/or firmware is deemed foreign-origin because of criterion (2) only, the Government shall have the right to require that the contractor not disclose the identity of the end user of the item to such individuals. In such a case, upon delivery of the software and/or firmware, the contractor shall certify that the identity of the end user was not disclosed to the individual(s).

Offeror must notify the Contracting Officer (CO) in writing at the time of submission of its proposal if any foreign-origin software and/or firmware will be included in the deliverables under the contract. When, after contract award, the contractor becomes aware of foreign-origin software and/or firmware to be delivered to the Government under the contract, the contractor shall immediately notify the CO in writing of the foreign-origin software and/or firmware to be included in the deliverables under the contract. Foreign-origin software and/or firmware that is merely a possible candidate for use under the contract shall also be identified.

Notification pursuant to this clause must include the identity of the foreign source and the nature of the software application, and is required as soon as there is a reason to know or suspect foreign-origin. Failure to provide adequate notice to the Government as specified herein can result in breach and/or default of the entire contract. If the CO does not reject foreign-origin software and/or firmware under this clause within 60 days of receiving notification, the Government's rights under this clause shall be waived.

10.2.3 Use of an Information Technology System to Support Contract Performance

Any information technology (IT) system utilized to support contract performance shall be operated in accordance with either the National Industrial Security Program Operating Manual (NISPOM) or the FBI Certification and Accreditation (C&A) Handbook.

It is a material condition of this contract that this clause be incorporated into any and all subcontracts. The certifying official as indicated on the DD Form 254 should be contacted to coordinate the required C&A process for contract performance.

Minimal requirements associated with the processing of FBI Sensitive But Unclassified (SBU), Law Enforcement Sensitive (LES), Limited Official Use (LOU), and/or For Official Use Only (FOUO) information are as follows:

1. The contractor shall designate, in writing, an individual to act as the Information System Security Officer (ISSO) responsible for this system/network.

2. The contractor is responsible for the security of all information systems used by the contractor, whether or not they connect to FBI networks, and are operated by the contractor for the FBI, regardless of location.

3. The contractor must not use or redistribute any FBI information processed, stored, or transmitted by the contractor except as specified in the contract.

4. The following constitutes the minimum set of technical security standards that must be applied to all information systems processing FBI information.

a. User Identification -- each system user shall have a unique user identification (UserId).

b. Authentication -- each system user shall be required to authenticate his UserId with a complex password.

c. Auditing -- each system shall be configured to perform auditing of system access. The following minimum information shall be captured in audit records.

(1) Identity of each user

(2) Time and date of each access

(3) Activities performed that might bypass, modify, or negate security controls

(4) Security-relevant actions associated with processing

d. Object Reuse -- each system shall clear memory and storage before reallocating space to a different user

e. Warning Banner -- a standard FBI warning banner shall be presented to each user when logging into any system processing FBI information

f. Inactivity Timeout -- an ADP system shall automatically revert to a secure condition if left inactive for a period of 15 minutes (or less) of inactivity, requiring the logged-on user to unlock the screen using a password

g. The contractor shall prepare and submit a System Security Plan (SSP) for review in support of a C&A effort.

10.2.4 Virus Control

a. The contractor certifies that it will undertake to ensure that any software to be provided or any Government Furnished Software to be returned under this contract, will be provided or returned free from any computer virus which could damage, destroy, or maliciously alter software, firmware, or hardware, or which could reveal to unauthorized persons any data or other information accessed through or processed by the software.

b. The contractor shall immediately inform the Contracting Officer when it has reasonable suspicion that any software provided or returned, to be provided or returned, or associated with the production may cause the harm described in paragraph (a) above.

c. If the contractor intends to include in the delivered software any computer code not essential to the contractual requirement, this shall be explained in full detail to the Contracting Officer.
d. The contractor acknowledges its duty to exercise reasonable care, to include the following, in the course of contract performance:

1. Using, on a regular basis, current versions of commercially available anti-virus software to guard against computer viruses when introducing maintenance, diagnostic, or other software into computers; and

2. Prohibiting the use of non-contract related software on computers, especially from unknown or unreliable sources.

10.2.5 Contracting Officer's Security Representative

Contracting Officer's Security Representatives (COSR) are the designated security representatives of the Contracting Officer and derive their authorities directly from the Contracting Officer. They are responsible for certifying the contraetor's capability for handling classified material and ensuring that customer security policies and procedures are met. The COSR is the focal point for the contractor, Contracting Officer, and Contracting Officer's Technical Representative regarding security issues. The COSR cannot initiate any course of action that may alter the terms or price/cost of the contract. The COSR for this contract is Joann Saunders and can be reached on (202) 220-9230.

11. Government Furnished Equipment (GFE)/Government Furnished Information (GFI)

11.1 Inventory Requirements

Special Provision H.15 Government Furnished Equipment, Information, or Services is applicable to this task order. Government Furnished Equipment and Information shall be returned to the Government at the completion of the task order unless otherwise directed.

11.2 Government Furnished Equipment

FBINet network and clients: SENTINEL will utilize the existing FBINet network and clients. The FBI will provide access to the FBINet and an interface to legacy systems (via the LAN at the Data Center). Available services include: WAN, LANs, Active Directory, MS Outlook, and PKI.

Enterprise monitoring system SENTINEL is to be integrated into the existing enterprise monitoring system managed by the Enterprise Operations Center (EOC). The SENTINEL system will supply network status and alerts to the EOC utilizing standard network monitoring components (listed in SOW Section 15.5.3). The contractor will be responsible for providing personnel responsible for monitoring the SENTINEL status. The contractor shall be responsible for purchasing and installing clients/agents on SENTINEL components as needed.

Enterprise licenses: COTS software for which an enterprise or site license exists may be made available. The Government will identify any available licenses that are relevant to the contractor's SENTINEL solution during final negotiations or after award. Adjustments to the Bill of Materials will be addressed at that time.

Operational facilities: Space and infrastructure support (power, cooling, communications) in existing operational facilities will be provided for the system. Space at the Clarksburg, WV Data Center will be provided for the primary and training systems. Space at the Washington D.C. Data Center will be provided for the backup and integration test system.

Communications: The Government will provide the following Communications conneetivity within 120 days, including encryptors, after the contractor's facility has met the DD Form 254 requirements:

- Communication link to Government systems and data as required for testing. The Government will supply the communications link and any required cryptographic equipment. The contractor is responsible for all routers, switches, etc. on its side of the interface.
- Communications link to FBI WAN for on-site Government access to email services and network.

11.3 Government Furnished Information:

- VCF IOC final report
- IPC and TNC definitions/descriptions/interfaees
- Non-commercial compliance and reference documents listed in this SOW
- Aecess to test data by TBS (*contractor to provide need dates*)
- Legacy system Interface Control Documents
- SUS Patch Management Roadmap
- Patch Management Overview
- Check for Available Patches
- Enclave/System Manager Approval
- Test Patch
- Deploy Patch
- Backout/Recovery and Reporting
- Notification Procedures

12. Packaging, Packing, and Shipping Instructions

The contractor shall ensure that all items are preserved, packaged, packed and marked in accordance with best commercial practices to meet the packing requirements of the carrier and to ensure safe and timely delivery at the intended destination. All data and correspondence submitted shall reference:

1. The CIO-SP2*i* Task Order Authorization Number
2. The NITAAC Tracking Number
3. The government end user agency
4. The name of the COTR

Containers shall be clearly marked as follows:

1. Name of contractor
2. The CIO-SP2*i* Task Order Authorization Number
3. The NITAAC Tracking Number
4. Description of items contained therein
5. Consignee(s) name and address

All commercial shipments to the JEH Building shall follow the instructions contained defined in the FBI Instruction: Commercial Delivery Instructions J. Edgar Hoover (JEH) FBI Building and Washington Field Office (WFO) dated 27 Dec 2000.

All shipments to Clarksburg, WV facility shall be addressed to:

1000 Custer Hollow Road
Clarksburg, WV 26306
Attn: Data Center

Shipping instructions for the Washington D.C. Data Center are located in the Commercial Delivery Instructions J. Edgar Hoover (JEH) FBI Building and Washington Field Office (WFO) dated 27 Dec 2000. Plan on an additional week beyond shipping time for commercial deliveries.

13. Inspection and Acceptance Criteria

Final inspection and acceptance of all work performed, reports and other deliverables will be performed at the place of delivery.

14. Accounting and Appropriation Data

Note that funds are not presently available for award of a contract at the time of issuance of this solicitation document. Therefore, the Government's intent to award a contract under this solicitation is contingent upon the availability of appropriated funds. No legal liability on the part of the Government can be incurred if an award is not made.

15. Other Pertinent Information or Special Considerations

15.1 Performance Criteria

The Award Fee Plan (AFP) defines the opportunity the Contractor has to earn fee commensurate with demonstrated performance. The Award Fee Plan has been developed to incentivize continuous Contractor responsiveness to program priorities and place an emphasis on quality program and technical management as well as cost and schedule savings. The Government will pay the Contractor an award fee for satisfactory or better performance. Notionally, the government anticipates capping the award fee pool for the development effort at 12% of development costs. Development costs are all costs incurred prior to each Phase Delivery Acceptance, not including equipment and "other direct costs". The award fee earned by the Contractor will be determined following suceessful completion of each Phase milestone event including: Initial Baseline Review (IBR), Critical Design Review (CDR), Operational Readiness Review (ORR), and Delivery Acceptance Review (DAR) for each phase. The government, at its sole discretion, reserves the right to roll unearned fee into any subsequent period within Phase; or into any subsequent Phase that has been contractually executed. Additional fee may be awarded for accelerated delivery as defined in Section 3 of the Award Fee Plan, Attachment 11. The fee structure is intended to encourage strong performance by the contractor in the highest risk areas. For more details on the government's perceived risk in each phase, accelerated delivery schedule, and the evaluation criteria for establishing the award fee, the Award Fee Plan (AFP) is provided in Attachment 11.
The performance requirements related to Award Fee Plan section 2.5.4.2-Technical Management and Performance for each task are contained in Table 15.1-1 below. Table 15.1-2 contains mandatory SLA content.

Table 15.1-1 Performance Requirements

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Acquisition Objectives	Phase deployments meet SOW acquisition objectives	Deployed Phases achieve Government's stated acquisition objectives (SOW para 3.0)	Government review of planned and actual Phase content.
SENTINEL Phase Capability Performance	Phase successfully completes all verification activities including: acceptance testing, security testing, and records management testing.	SENTINEL system level acceptance testing in an operating environment at a designated FBI facility meets the functional and performance standards established in the SRS and allocated to that Phase. Record management certification and Approval to Operate are achieved.	Government assessment of Phase test data and test reports.
Systems Engineering Execution	SENTINEL successfully passes its required LCMD gates and project reviews per Phase.	Phase's LCMD control gates and project reviews successfully completed using the entrance and exit criteria established in the IMP. The Government shall be final approval authority as to a successful gate/project review event.	Government assessment of LCMD gate and project reviews.
Architecture Qualities	The SENTINEL architecture is scalable, robust, and flexible. The architecture complies with the FBI Enterprise Architecture. The architecture reflects a modular approach that embraces encapsulation of functionality. The architecture supports easy integration among components and products that were not neeessarily originally designed to work together. The architecture facilitates changes to be accommodated in a manner such that changes propagate to as few other components as possible.	100% compliance is required.	Government analysis of architecture products, modules, and interfaces to assess descriptions, definitions, attributes, use of rules and conventions for standards compliance, product consistency, communicability, and implementation viability.
Information Sharing	The architecture facilitates information sharing by using Government standard XML schema definitions where appropriate to interface with external	100% compliance is required.	Government analysis of architecture, modules, and interfaces.

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
	systems that will support the rapid exchange of electronic information with External Agencies. The architecture has a single point of access to investigative information within the FBI. The architecture supports common standards for information sharing, as delineated by the contractor.		
Phase data migration	All necessary data is migrated from each legacy system. Each migrated data set is complete and accurate. "Data" not meeting the SENTINEL data standards is flagged and provided to the Government for action.	100% compliance is required.	Government review and independent verification and validation of data migration test results.
Phase schedule and file plan data	Government approved, complete and accurate schedule and file plan data are loaded in the system. Delivered records management capability is fully operational.	100% compliance is required.	Government review of product. Government monitoring of system level tests. Independent verification and validation results review.
Phase technical data package	The technical data package is complete and accurate, reflecting the as delivered system configuration. Documentation for the system administrators is complete, accurate and easy to use.	100% compliance is required.	Government review of contractor audit records. Government review of configuration audits. Independent verification and validation. Government Functional and Physical Configuration Audits.
O&M Training	System Administrators, privileged users, and help desk operators shall receive training and training materials appropriate for their intended use of the system.	Training materials are clear, concise, correct, and use color diagrams to lead the user through the learning process. Users can perform all routine tasks at the completion of training (includes a combination of classroom training, on-the-job training, and reading of baseline procedures, manuals, and guidebooks).	Government review of training materials. Government monitoring of courses. Government monitoring of student evaluations.
Service Level	The system is operated and	100% compliance is required.	Review of: trouble tickets,

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Agreements	maintained at the levels specified in the Government approved Service Level Agreement.		contractor maintenance logs, and contractor incident tracking reports.
User Training	System users shall receive training and training materials appropriate for their intended use of the system.	Training materials are clear, concise, correct, and use color diagrams to lead the user through the learning process. System users can perform all routine operations at the completion of training (includes a combination of classroom training, on-line training, and reading of guidebooks).	Government review of training materials. Government monitoring of courses. Government monitoring of student evaluations.
Organizational Change Management	User Communities – agents, analysts, professional staff, O&M staff are well informed of and accept each Phase's deployed capabilities.	User Communities – agents, analysts, professional staff, O&M staff, are participants during SENTINEL development, deployment, and employment. Their concerns and issues are responsively and effectively addressed	SENTINEL's User Advocate Team assessment and Deployment Readiness Review results
Users employment of Phase's capability	User Communities – agents, analysts, professional staff, O&M staff are well trained and can effectively and efficiently use a Phase's set of capabilities	Users self-report work productivity improvement.	SENTINEL's User Advocate Team assessment based on Field Offices and Hq inputs.

Table 15.1-2 Mandatory SLA Content

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Updates and Patches	Updates and patches are implemented within one week of approval by the Configuration Control Board.	100% compliance is required unless a Government waiver of the requirement is approved.	Audit of configuration management logs. Monitoring of operations and maintenance activities.
Maintaining System Security	System security is maintained at the certified level using the baselined security documentation. The security documentation is kept up to date using the baselined configuration management procedures to reflect any security related changes to the system.	100% compliance is required.	Review of the security documentation. Audit of configuration management logs.
Asset	All assets are accounted for	Assets changes are logged	Audit of inventory records

Item of Interest	Desired Outcome	Performance Standard	Monitoring Method
Accounting and Inventory	and an up to date inventory is maintained.	within 24 hours of arrival/departure.	and inventory.
Periodic Maintenance	Periodic Maintenance for hardware shall not exceed 2 hours/week	100% compliance is required.	Audit of maintenance logs
Vendor Response Time	The ITOD's Data Center Unit (DCU) requires a one hour response time for vendor support	100% compliance is required.	
Problem Ticket/System Defect Response time	EOC response timelines are met/supported	Critical = Acknowledged in 15 minutes, problem resolved within 2 days High = Acknowledged in 24 hours, problem resolved within 4 days Medium = Acknowledged in 48 hours, problem resolved within 5 days Low = Acknowledged in 72 hours, problem resolved within 6 days	Review of ServiceCenter™ logs

15.2 Organizational Conflict of Interest (OCI) Mitigation Plans

Every contractor or subcontractor who submits an offer as a prime contractor or as a member of a contractor teaming arrangement shall review and comply with FAR Subpart 9.5. Each of the items listed below shall be specifically addressed corresponding to the unique numeric designation.

1. Organization charts showing the company's corporate structure and highlight elements of the company participating in the contract.
2. Demonstrate how the elements performing the proposed effort will be isolated from the remainder of the company.
3. Describe how information, whether in hard copy or electronic media, will be stored and destroyed in order to preclude a transfer of information.
4. Describe how networks and servers will be protected to prevent unauthorized transfer of information.
5. Describe management reporting chains in sufficient detail to demonstrate that the proposed effort and decisions related to the effort will be isolated from the remainder of the company.
6. Address how your company will preclude a perception of impaired objectivity.
7. Provide information to indicate if the organizational elements performing the proposed effort will be geographically or physically separated from the remainder of the company.
8. Deseribe techniques your company will employ to mitigate the perception that you will favor your own products or services.
9. Describe the proeess in which the government will have insight or oversight of key processes.
10. Describe any situation in which management outside the mitigated organization will have access to key decisions for which the mitigated organization is responsible.
11. Provide all documents that your employees are required to sign indicating, which employees are required and how often the requirement is.
12. Describe the process for reassigning personnel, including subcontractors, from one assignment to another, include restrictions.

13. Describe the process for employees that leave your employment and any control you exercise over their future employment, particularly as it relates to OCI and non-disclosure.
14. Describe any OCI training your employees are offered and or mandated, along with the timing (before or after starting work on a government contract) frequency, length and content of such training.
15. Describe if your company conducts self-audits and if they will be made available to the government.
16. Describe the proposed process and timeline for submitting, and obtaining the approval by the Contracting Officer, of the OCI Mitigation Plans for any and all subcontractors added to the contract post award that were not included in the OCI Mitigation Plans submitted as part of the contractor's proposal.

To enable the Government to fairly evaluate the proposed plan, the following shall be specifically addressed:

A. Disclosure of business activities of your company, your affiliates, your team members and affiliates of your team members which create either a conflict of interest or the appearance of a conflict of interest.
B. Provide evidence of facts and circumstances that you believe mitigate or address concerns related to the appearance and/or presence of an OCI.
C. Explain your proposed approach to mitigating the effects of any apparent or actual conflicts of interest arising out of the business activities disclosed in response to (A.) above.

The government will treat all submissions as proprietary under 18 U.S.C. §1905 and protect proposed information accordingly.

15.3 Reserve

15.4 Contractor Travel

All travel must be pre-approved by the COTR in writing and must comply with the Federal Travel Regulation.

15.5 SENTINEL Standards

15.5.1 Usability Standards (TBR):

- ISO 13407:1999 - "Human Centered Design Processes for Interactive Systems"
- ISO 11581 - "Icon Symbols and Functions"
- Microsoft GUI guidelines

15.5.2 Development Standards:

The FBI prefers use of these tools however compatible alternatives are acceptable:

- Popkin System Architect
- Popkin Integrated Reference Model Application
- AllFusion® ERwin Data Modeler

15.5.3 Operations and Maintenance Standards

The following are a list of the products and services used by ITOD:

- Peregrine's Service Center™ is utilized for Change Management, Security Access Request (SAR), SLA Tracking, and generating Trouble Tickets. It assists with the tracking and the approving of changes to the FBI's IT environment for network and baseline software changes, file changes, application software changes, etc. Recording and tracking processes for Commercial Off-the-Shelf (COTS) software is another utilized feature of Peregrine's Service Center™.

- RATIONAL (i.e. ClearQuest™, ClearCase™) is being utilized by the FBI to perform modeling, version control of software and documents, defect workflow/tracking, enhancement request workflow/tracking, testing, performance testing, and requirements tracking. This tool shall be utilized by the development team and transitioned to ITOD for O&M purposes.

- Enterprise standards (commercial software products) for network monitoring and management are listed below. The FBI prefers use of these tools. The Offeror may select comparable products provided they interface to Micromuse's Net Cool and they provide justification for the selection.

  - HP Openview (enable SNAP traps and queries)
  - NetIQ – Application Manager (server agent)
  - NetIQ – Security Manager (server agent)
  - E-Policy Orchestrator (McAfee NetShield)
  - Tripwire (server agent)
  - Navisphere (agent for EMC SAN management)
  - Micromuse Net Cool (enable SNAP traps and queries)
  - SMS Agent (agent for remote management)
  - Antigen (email antivirus) (server agent)
  - Veritas Netbackup (backup management) (server agent)
  - Infovista (performance management) (SNMP traps)
  - CiscoWorks (configuration management) (SNMP traps)
  - RSA ACE (authentication) (syslog messages)
  - Cisco Secure ACS (Cisco access control) (syslog messages)
  - Dell OpenManage Suite (Hardware Health monitoring of all Dell Servers).
  - Native Windows 2000 Server tools (e.g. Cluster Administrator, AD Users & Computers). More detailed applets used to monitor smaller pieces of the enterprise when needed.
  - NetIQ DRA (3rd party tool used in place of Active Directory Users and Computers, used more for troubleshooting than monitoring).

  At the time of contract award through the period of performance, in the event that enterprise standard software packages for network monitoring and management encounter changes, the vendor is expected to factor into the contract operations and maintenance the need to train their technicians accordingly to provide the same level of response to all software changes at no additional charge.

- The FBI's current VIRUS Protection Software shall be used to the extent possible.

- The SENTINEL client "applications" shall run on FBI approved desktops.

15.6 Government Space at Contractor Facility

Although some work will be accomplished at FBI facilities, the primary site for work associated with this Task Order shall be the contractor's facility. The contractor shall support frequent short notice meetings and briefings at FBI Headquarters and other locations in the Washington, D.C. metropolitan area.

The contractor provided facility shall contain sufficient floor space to house contractor personnel, government personnel (15), computer systems and components. The facility shall support both Unclassified/For Official Use Only (FOUO) and Secret. The two enclaves shall be separate and distinct

from each other as well as any corporate network. It is anticipated that the activities such as document development, purchasing, and program management will be housed on the Unclassified/FOUO network. The Secret network shall host the development, test, integration of the new system and the FBINet for communications, email, and document exchange.

15.7 Installation Support

The Government will provide the operational and backup facilities. Workspaces for TBS *(offeror to supply requirement as part of proposal)* operations and maintenance personnel will be provided. The contractor shall be responsible for all cable and cable pulling activities from the agreed to interface to and between the delivered equipment. Standards for the facilities are contained in the ITOD Data Unit, Equipment Installation Standards and ITOD Data Unit, Equipment Installation Standards (Clarksburg, West Virginia)documents.

15.8 Key Personnel

Key Personnel considered essential to the performance of this Task Order are:

- Task Order Program Manager
- Task Order Deputy Program Manager
- Task Order System Chief Engineering and Architecture Manager
- Task Order System Test Manager
- Task Order Certified Records Manager *
- Task Order Security Engineering Manager
- Task Order Organizational Change Training and Transition Manager

*Certification via Institute of Certified Records Manager. Equivalent qualifications may be considered.

Key Personnel Qualifications are provided at SOW Attachment 4-Key Personnel Duties and Qualifications.

15.9 Software Licenses

If development tools are proposed that require licenses/seats for Government use, 15 seats for Government use shall be purchased.

15.10 Development Environment

If not available through an existing FBI enterprise license agreement, hardware and software used in the development of the system shall be procured under this contract and delivered to the Government at the completion of the contract. All licenses and warranties purchased under this contract shall be transferable and shall be transferred to the Government at the completion of the contract or upon Government request.

The development environment includes all strings used to develop and operate SENTINEL including unclassified and classified development, integration and test, staging, operations, backup, and training strings.

15.11 Applets, Plug-ins and Other Applications Planned for FBINet

Any applet, plug-in or other applications that will be pushed to or reside on FBINet clients require Government approval. Descriptions of any proposed applet, plug-in or other applications shall be identified to the Government no later than PDR.

15.12 Software Engineering Institute (SEI™[2]) Capability Maturity Model Integration (CMMI®[3]) Level 3 Requirement

The contractor, including all organizations and subcontractors that will be contributing a minimum of 10% of the total SENTINEL level of effort developing or integrating software, shall perform the task order activities in accordance with the processes assessed at an SEI CMMI (or equivalent) Level 3 as presented in the proposal. The Government reserves the right to conduct independent assessments during the period of performance to verify compliance with established processes. In the event that the contractor provided a risk mitigation plan, an implementation plan, and a schedule for achieving full compliance in lieu of an existing CMMI Level 3 assessment, the Government reserves the right to conduct independent assessments to verify achievement of the Level 3 processes.

15.13 Vendor Contracts for Operations and Maintenance

The contractor and the Hardware/Software Vendors must have agreements that specifies the following: Local service personnel availability and backup resources; test equipment and services; provide all current and revised test equipment (i.e. hardware, software, and firmware); maintenance and escalation plans during bi-annual meetings between the FBI and the contractor; the ability to work with other vendors for solutions when necessary; the ability for the original equipment manufacturer to inspect government equipment for mandatory engineering change orders to upgrade equipment; vendor provided computer engineers/technicians that have expert level experience in maintaining the same or similar equipment. Ensure that parts are included as a mandatory requirement for hardware maintenance.

15.14 Mandatory Patch Management Procedures

The Software Update Services (SUS) Patch Management Process is contained in the SUS Patch Management Process document. The SUS Roadmap and Patch Management Overview documents provide a description of the Patch Management Process for implementing software patches within any network in the FBI headquarters. This guidance shall be followed when conducting patch management on any SENTINEL operational system. Process documents are:

- SUS Patch Management Process
- Check for Available Patches
- Enclave/System Manager Approval
- Test Patch
- Deploy Patch
- Backout/Recovery and Reporting
- Notification Procedures
- SUS Roadmap
- Patch Management Overview

15.15 Release Information – Publications by Contractor Personnel

The Federal Bureau of Investigation (FBI) specifically requires that Contractors shall not divulge, publish, or disclose information or produce material acquired as or derived from the performance of their duties.

---

[2] (SM) SEI is a service mark of Carnegie Mellon University

[3] ® CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

For purposes of this Clause, "Information" shall include but not be limited to: in any media or all media including on the web or web sites; publications, studies, books, theses, photographs, films or public announcements, press releases describing any part of the subject matter of this contract or any phase of any program hereunder, except to the extent such is:

(i) already known to the Contractor prior to the commencement of the contract
(ii) required by law, regulation, subpoena or government or judicial order to be disclosed, including the Freedom of Information Act.

No release of information shall be made without the prior written consent of the Office of Public Affairs and the Contracting Officer. The contractor and author are warned that disclosure is not without potential consequences. The FBI will make every effort to review proposed publications in a timely manner to accommodate these and other publications.

Where appropriate, in accordance with established academic publishing practices, the FBI reserves the right to author/co-author any publication derived from this contract.

These obligations do not cease upon completion of the contract.

15.16 Privacy Act

All contractors and subcontractors shall comply with 5 USC 552a(m) of the Privacy Act which reads as follows:

"(m) Government contractors

(1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i)[4] of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under Section 3711 (e) of Title 31 shall not be considered a contractor for the purposes of this section"

16. Post-Award Administration

The Government will monitor the contract performance using the contractor provided IMP and IMS. Milestones and work activities along with LCMD control gates and reviews shall be monitored following the performance criteria in the Award Fee Plan at Attachment 11.

Critical Path Management (CPM) will be used as the primary schedule and cost control mechanism. Progress will be measured using Earned Value Management (EVM). The Government will be using Microsoft Project 2003 Professional and Metier's WorkLenz™5 software package to monitor schedule and earned value performance and report on that performance up through the OMB Exhibit 300 reporting cycle. The contractor shall be required to submit data at least monthly in electronic formats suitable for uploading into the Government's MS Project and WorkLenz project files.

[4] Section (i) has criminal penalties – misdemeanor and $5,000 fine

The Government will complete award fee evaluations following process and schedule defined in the Award Fee Plan in Attachment 11.

In accordance with NIH SP2 requirements, the Govemment will complete Past Performance Evaluations at least annually and at the end of the task.

17. Evaluation Criteria

Award of the SENTINEL Task Order will be made to the Contractor whose proposal, conforming to this solicitation, is determined to be the best value to the Government using the "Best Value" process as defined in FAR 15.101-1. This process permits trade-offs between cost or price and non-cost considerations and allows the Government to accept other than the lowest priced proposal. In such an occurrence, the perceived benefits of the higher priced proposals shall merit the additional cost.

The Technical Approach and Management Approach evaluation items are of equal importance. Both Technical and Management Approach items, individually, are more important than the Past Performance item. The Security Approach and OCI Mitigation evaluation items will be assessed on a Pass/Fail basis. Failure of either of these items may result in the offer being removed from consideration. The Past Performance, Technical Approach and Management Approach evaluation items, when combined, are significantly more important than Cost. In the case of essentially equal and acceptable evaluation of Past Performance, Technical Approach and Management Approach, Cost will assume greater importance, and may become the determinative factor for making award.

Note that funds are not presently available for award of a contract at the time of issuance of this solicitation document. Therefore, the Government's intent to award a contract under this solicitation is contingent upon the availability of appropriated funds. No legal liability on the part of the Government can be incurred if an award is not made. Award will be made to the Offeror proposing the solution most advantageous to the Government based upon an integrated assessment of the evaluation Items and Factors listed below, cost and other factors considered. The SENTINEL evaluation criteria for award are:

I. Past Performance Item

This evaluation item examines the quality of the Offeror's past performance on programs that are similar in size, scope and technological and managerial complexity to the SENTINEL program. The Government will evaluate the quality of the Offeror's past performance and reserves the right to seek out past performance information in addition to that provided in the proposal, from any and all sources both inside and outside of the Government, and to use the information received in the evaluation of past performance. These cited programs must be appropriately recent and relevant in order to receive favorable consideration. In determining the rating for the past performance evaluation factor, the Government will give greater consideration to the Offeror's performance under the contracts which the Government feels are most relevant to SENTINEL. This item includes assessments of Technical Past Performance, Management Past Performance, and a Demonstration of one of the fielded systems cited in the Offeror's Past Performance volume.

Factor 1: Technical Performance
This factor evaluates the quality of the Offeror's technical performance on recent and relevant programs. The factor addresses the adequacy of the Offeror's demonstrated capability in developing and deploying technology that is applicable to the SENTINEL program. Included in this factor will be an assessment of the Offeror's success in meeting program performance requirements using a phased development approach, integrating COTS/GOTS products at the enterprise level, and migrating legacy data and applications.

Factor 2: Management Performance
This factor evaluates the quality of past management performance on recent and relevant programs. The factor addresses the adequacy of the Offeror's demonstrated performance in

managing and executing recent and relevant programs that are applicable to the SENTINEL program. Included in this factor will be an assessment of success in meeting schedule requirements, cost control requirements and program planning and execution.

Factor 3: Past Performance System Demonstration
This factor evaluates the quality of the performance of a deployed system that the Offeror has developed and believes to be of relevance to the proposed SENTINEL functionality. Included in this factor will be an assessment of the quality of the deployed system's implementation of key SENTINEL functionality, to include any or all of the following:

- Case Management
- Document Management
- Document Authoring
- Evidence Management
- Records Management Application (RMA) or Electronic Records Keeping (ERK)
- Security (Discretionary Access Control, Role-Based Access Control)
- Workflow

II. Technical Approach Item

This evaluation item examines the quality of the Offeror's proposed technical approach to meeting the SENTINEL performance requirements. This item includes assessments of the quality of the Offeror's proposed SENTINEL solution and of their phased development approach.

Factor 1: Proposed Technical Solution
This factor evaluates the quality of the Offeror's technical solution as evidenced by their description of an adequate systems architecture and system design. The factor also evaluates the sufficiency of the proposed COTS/GOTS selection approach and identification, as well as the adequacy of the proposed solution's scalability, maintainability and security attributes. This factor also addresses the quality of the Offeror's approach to legacy data migration and legacy application transition.

Factor 2: Phase Development Approach
This factor evaluates the quality of the Offeror's phased development approach as evidenced by their description of an adequate system development approach. The factor also evaluates the sufficiency of the proposed Integration and Test approach, as well as the adequacy of the proposed technical deployment approach and pre-FOC Operations and Maintenance strategy.

III. Management Approach Item

This evaluation item examines the quality of the Offeror's proposed management approach for executing the SENTINEL design, development, integration and test, deployment, and operations and maintenance. This item includes assessments the quality of the Offeror's Executive Overview, proposed program organization, Systems Engineering approach, appropriateness and quality of their Team composition, and quality of the organizational change management strategy.

Factor 1: Executive Overview (Oral Briefing)
This factor evaluates the Offeror's understanding and overall approach to satisfying the requirements of the TORP. It includes an assessment of the Offeror's proposal strengths and capabilities, excluding cost/price, as well as the proposed solution to managing technical processes.

Factor 2: Program Organization
This factor evaluates the quality of the Offeror's proposed strategy for managing the SENTINEL program development activity. Included in this assessment is an evaluation of the quality of the

Offeror's proposed Integrated Master Plan, the adequacy and realism of their proposed program schedule, the adequacy of the Offeror's implementation and traceability of SOW requirements, their proposed staffing approach and the adequacy of the Offeror's strategy for identifying, mitigating and managing SENTINEL programmatic and technical risk.

Factor 3: Systems Engineering
This factor evaluates the quality of the Offeror's proposed systems engineering methodology and the appropriateness of the tailoring of that process for the SENTINEL program. It also evaluates the adequacy of the Offeror's systems engineering processes as they are applied to their proposed solution.

Factor 4: Team Composition
This factor evaluates the quality of the Offeror's proposed corporate skills and abilities represented on their proposed SENTINEL team, and the appropriateness of their team composition in light of the stated goals and objectives of the SENTINEL acquisition. Included in this factor is an assessment of the qualifications of the Offeror's proposed Key Personnel, the ability of their Team organization and roles and responsibilities to adequately ensure an efficient and effective fit within the overall government organization, and of the adequacy and appropriateness of the proposed Team's domain knowledge.

Factor 5: Organizational Change Management
This factor evaluates the quality and effectiveness of the Offeror's proposed Organizational Change Management (OCM) strategy. Included in this factor is an evaluation of the Offeror's proposed methodology and approach to ensuring user acceptance through ongoing communications, program advocacy and marketing and the development and deployment of training. Also included in this factor is an assessment of the Offeror's transformation approach, which must demonstrate an adequate understanding of the business changes associated with SENTINEL and describe a plan for mitigation of user resistance.

IV. Security Approach Item (Pass/Fail)

This evaluation item examines the quality of the Offeror's proposed approach for meeting the SENTINEL security requirements. This evaluation item encompasses the evaluation of four factors for award: Personnel Security, Infrastructure Security, Lifecycle Security, and Acquisition Risk Assessment. Evaluation of these factors is Pass/Fail. Failure to meet these the standards of these evaluation factors may result in the Offeror's proposal no longer being considered for award.

Factor 1: Personnel Security
The Personnel Security Factor evaluates the Offeror's compliance with personnel security requirements for the SENTINEL program. Included in this evaluation will be a verification of the status of the proposed cleared personnel at contract award in accordance with the appropriate FBI Security policies and the SENTINEL SOW, the Offeror's willingness to participate in the FBI's polygraph program, as well as an assessment of the adequacy of the Offeror's proposed plan of action for augmenting their cleared labor pool beginning at contract award to meet SENTINEL requirements for appropriately cleared personnel.

Factor 2: Infrastructure Security
The Infrastructure Security Factor evaluates the Offeror's compliance with infrastructure security requirements necessary to support the SENTINEL program. Included in this evaluation will be a verification of the status of the proposed accredited Offeror facilities at contract award in accordance with the appropriate FBI Security policies and the SENTINEL SOW. This factor will evaluate the adequacy of the Offeror's plan for providing an FBI-accredited development environment that meets the facility requirements of the SENTINEL SOW at the time of contract award, or a plan for how these requirements will be met. This factor also includes an assessment of the Offeror's plan for complying with FBI security requirements for the processing of

SENTINEL program data on automated information systems within the Offeror's development environment.

Factor 3: Lifecycle Security

The Lifecycle Security Factor evaluates the quality of the Offeror's plan for identifying and incorporating appropriate security measures throughout the SENTINEL program lifecycle. Included in this evaluation will be an assessment of the Offeror's proposed approach for maintaining compliance with, and staying abreast of all appropriate FBI security policies and directives. This includes the corporate commitment for staffing SENTINEL tasks with appropriately cleared personnel, maintaining accredited facilities, and implementing a robust security management plan for teammates and subcontractors.

Factor 4: Acquisition Risk Assessment

The Acquisition Risk Assessment Factor evaluates the risk posed to the government by the Offeror of the SENTINEL acquisition. Included in this evaluation will be an assessment of the Offeror's Certificate Pertaining to Foreign Interests (SF 328) and Key Management Personnel List (KMPL), particularly the impact of any Foreign Ownership Control or Influence (FOCI) on their organization or activities, or the organization or activities of a subcontractor.

V. Organization Conflict of Interest Item (Pass/Fail)

The Organizational Conflict of Interest (OCI) Mitigation Item evaluates the Offeror's proposed plan for mitigating any and all real or perceived organizational conflicts of interest. The evaluation criterion is met when the Offeror's OCI Mitigation Plan describes an acceptable approach to identifying, avoiding, and mitigating organizational conflicts of interest. Evaluation of this item is Pass/Fail. Failure to meet this criterion may result in the Offeror's proposal no longer being considered for award.

VI. Cost/Price Item

The Cost Item evaluates the Offeror's proposed cost for realism, reasonableness and completeness. The objective of proposal cost analysis is to ensure that the final agreed-to price is fair and reasonable. Cost information may be provided to members of the Non-Cost evaluation team in accordance with agency procedures in order to provide greater expertise to the Cost evaluation team. The Cost evaluation process does not result in a qualitative rating, as does the non-cost evaluation. Rather, the Offeror's proposed cost is analyzed and any noted discrepancies in cost realism, cost reasonableness and cost completeness are noted and are communicated to the SSA during the SSET's Award Recommendation Briefing.

Factor 1: Cost Realism

The Cost Realism evaluation includes a review of the technical and management volumes and Offeror Bases of Estimate (BOEs) to determine if these approaches, and their corresponding cost estimates, are realistic for the work to be performed, reflect an understanding of the requirements, are consistent between the various elements of the proposal, and if the proposal can executed for the proposed cost.

Factor 2: Cost Reasonableness

Cost Reasonableness is assessed by reviewing the proposal Basis of Estimates (BOEs) to determine the confidence of the estimating methods used to substantiate the proposed costs. According to FAR 31.201.1, an Offeror may use any generally accepted estimating method that is equitable and consistently applied. Normally, adequate price competition establishes price reasonableness FAR 15.403-1 c.1.

Factor 3: Cost Completeness

Cost/price proposals shall be evaluated for completeness by assessing the responsiveness of the Offeror to the solicitation requirements. For the cost data to be complete, the Offeror must provide all data that is necessary to support the offer.

18. Data Item Descriptions

Data item descriptions are located in the FBI LCMD Appendix H and the FBI Certification and Accreditation Handbook except as noted below. In the event that a description is provided in the SOW and in one of the two referenced documents, the SOW description shall take precedence.

18.1 Task Order Management Plan

This is the first plan for the project. The Task Order Management Plan (TOMP) provides high-level planning information and is supplemented by other, more detailed planning documents as the project proceeds through its life cycle.

1.0 Introduction

1.1 Document Overview

A Document Overview section shall summarize the purpose and contents of this document.

1.2 Program Overview

The Program Overview shall identify the name of the project and it shall identify the FBI is the acquiring entity. The Program Overview shall briefly state the purpose of the project.

2.0 Referenced Documents

This section shall list the number, title, revision, date, and originating organization of all documents referenced in this document.

3.0 Program Requirements and Objectives

This section identifies the system requirements and project deliverables.

Identify system requirements in priority order. Reference to the System Requirement Document is acceptable. Identify driving operational need dates or ties to external milestones, which may influence the structure and scope of the project. Identify the capacity that must be obtained to meet operational requirements.

List those items that the project is expected to deliver or place into operations. This may include functional capabilities, support infrastructure, number of units, documentation, and training.

4.0 Organizations

Provide a list of organizations that will be involved in the project. Identify the organizations including subcontractors, the scope and amount of effort that each organization must contribute by Phase, SOW task and subtask, and the Point of Contact (POC) in each organization. Provide a Key Management Personnel List (KPML).

5.0 Program Monitoring and Control

This section defines level of monitoring and control that will be implemented on the project.

5.1 Level of Configuration Management

Describe the techniques to ensure configuration management.

5.2 Level of Reporting and Monitoring

Describe processes to be used to monitor and report on project status and risk. Describe the Earned Value Management process to be applied on the project. Describe the measurement program. Describe the readiness planning and review process for the development and its assorted documentation based on the project level reviews and control gates defined in the SOW.

5.3 Quality Assuranee

Describe how quality practices will be implemented, assessed, and monitored. Describe the metrics that will be used to monitor the success of the project as it moves through its life cycle.

6.0 Security

Describe the security process that will be implemented on the project. Define how system security is to be addressed, including accordance with the Systems Engineering Management Plan (SEMP). Describe any special personnel security considerations of the project.

7.0 Notes

This section shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

A. Appendices

Appendices may be used to provide information published separately for convenience in document maintenance (e.g., charts, classified data). As applicable, each appendix shall be referenced in the main body of the document where the data would normally have been provided. Appendixes may be bound as separate documents for ease in handling. Appendixes shall be lettered alphabetically (A, B, etc.).

18.2 In Progress Review Report (monthly)

The In Progress Review Report is the organized documentation of proceedings of the monthly In Progress Review. The report is a compilation of briefings, handouts, and action items given at the review. Contractor formatting of briefings, handouts, and action item lists is acceptable provided that Government has not made prior restrictions in the statement of work or other data item descriptions. Contractor formatting of the report is acceptable. The In Progress Review Report shall be delivered to the Government in a Government-approved electronic format. The content of the In Progress Review Report shall include the following information in the order specified:

1. Title page
2. Brief statement (no more than one page) by the program manager summarizing the state and issues facing the program
3. Table of Contents
4. Listing of pages in the report that were changed (additions, deletions, or modification) from what was presented or distributed at the Review and a description of each change (e.g., if 5 changes were made on a page, each change must be described). Changes must be indicated on the affected page. (It is the expectation that there will be few, if any, changes between the review and the delivery of the report, and that any changes be significant.)
5. In Progress Review Action Item List (to include date opened, action, assignee, status, and date closed)
6. Required topical summaries (each summary listed in table of contents):
    - Earned value
    - Schedule
    - Funding and obligations
    - Subcontracts
    - Risks
    - Program and risk management metrics as required by the Measurement Plan
    - Quality assurance
    - Configuration management
    - Security management applied to task order
    - Staffing plan
    - Phase Development Status
    - Operations and Maintenance Status
    - OCM Status
    -
7. Other topics (each topic listed in the table of contents)

IPR briefing charts are to be provided two working days in advance of the meeting. The IPR Report is to be delivered within 3 working days following the meeting.

18.4 Contract Funds Status Report

The contractor will complete DD Form 1586, Contract Funds Status Report, subject to the latest available version of the Contract Funds Status Report Data Item Description DI-MGMT-81468.

18.5 Earned Value Management System (EVMS) Report

Earned Value Management System (EVMS Report)	Item Number: **18.5**
	Revision #: R01
	Effective Date: 05-27-04

Use

This written document and the associated electronic deliverable provide detailed earned value management system (EVMS) information on the combined cost, schedule, and earned value performance through the proceeding Gregorian calendar month against a project's EVMS Baseline. The information is clearly differentiated so as to provide visibility of the project's performance as a whole against the total EVMS Baseline and the project's performance against the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

Interrelationship

The written document and the associated electronic deliverable are delivered to the Program Manager and the Contracting Officer (if the project is part of a contract) with the EVMS Plan, EVMS Implementation Plan (as required), Work Breakdown Structure (WBS), Integrated Master Schedule (IMS), Control Account Funding/Spend Plans, Work Authorization Document(s), Subcontractor Management Plan, EVMS Baseline, and Updated Risk Assessment as required in the Program Plan and/or Contract Statement of Work as appropriate.

Preparation information

Preparation of the written EVMS Status report

A Written EVMS Status Report will be prepared and submitted (typically by the 15th of the following month) that summarizes the EVMS performance through the end of the month immediately preceding the report.

The EVMS parameters reported are generally based on the cumulative Budgeted Cost of Work Scheduled (BCWS), Budgeted Cost of Work Preformed (BCWP), and Actual Cost of Work Performed (ACWP) to date. BCWS and BCWP data shall be budgeted and captured at the lowest available level of the EVMS Baseline, which is typically at the work package level, and rolled up to level 1 of the WBS. ACWP shall be budgeted and captured at the lowest available Control Account level of the WBS and rolled up to level 1 of the WBS.

The report shall be addressed to the Program Manager and, if appropriate, the Contracting Officer. Program stakeholders that will have access to the report include:

- The Program Manager
- The Contracting Officer
- Designated Members of the Govern ment's Program Management Team, including contracted support staff.
- FBI Executives
- All appropriate external stakeholders, including OMB.

1.0 Introduction

The introduction to the report will identify the approval or draft dates of the EVMS baseline being reported against and identify any approved Change Requests that may have been used to modify the Baseline since the last report. The report follows with the 6 sections identified below.

2.0 EVMS Graphs

Two graphs will be presented that show the BCWS, BCWP, ACWP, EAC1, and EAC2 at WBS Level 1, as monetary figures (y-axis) against Gregorian calendar months (x-axis). One graph shall be for the whole EVMS Baseline. The second graph shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

3.0 Historical Tables of Summary EVMS Parameters

Two tables of summary EVMS parameters for the last 6 months shall be presented. Each table shall include BCWS, BCWP, ACWP, VAC1, VAC2, CV, CPI, SV, and SPI at WBS level 1. One table shall be for the whole EVMS Baseline. The second table shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

4.0 Historical Tables of Summary Work Package Status

Two tables showing a summary of the status of EVMS deliverables (work packages), by calendar month, from project start through the current month shall be presented. For each calendar month since project inception through the current month being reported on, each table should list:

- The total number of deliverables due to date (to have been started by the end of the month)
- The total number of deliverables that are "on schedule" as of the end of the month.
- The total number of deliverables that are "late" as the end of the calendar month.
- The total number of deliverables reported as "late" in the previous month that are now completed and/or "on schedule"

One table shall be for the whole EVMS Baseline. The second table shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology.

5.0 Detailed Table of Late Deliverables/Work Packages

A single table listing each deliverable/work package that is now "late" as of the end of the calendar month shall be presented. The information for each deliverable shall contain the following information:

- The calendar month that the deliverable/work package was due to have been started or finished
- The WBS Number
- The responsible party
- The name/title of the deliverable/work package

- The reason that the deliverable/work package is late (either "Late Start" or "Late Finish".)
- The methodology being used to measure work package value (E. G. LOE, 0/100, 20/80, or 50/50).

6.0 Narrative Analyses

This section shall provide two narrative analyses of EVMS performance to date. One narrative analysis shall be for the whole EVMS Baseline. The second narrative analysis shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology. Each narrative analysis shall be further divided into three parts. They are:

6.1 Variance Analysis

This is a narrative discussion of the cost and schedule variances at WBS level 1. The discussion includes, this month's variances, last month's variances, reasons for the variances, and what WBS level 2 items have negative cost and schedule variances.

6.2 Overall Performance

This is a short, high-level, summary discussion of the overall EVMS performance of the project. It includes short, high-level, summary recommendations on how to improve future EVMS performance (e.g. use management-by-exception techniques to focus team performance on completing the late deliverables/work packages.) It also includes a discussion of the calculated variances at completion (EAC1 and EAC2) based on CPI and a CPI/SPI combination.

6.3 Estimate at Completion

This is a short, high-level, summary discussion/prediction about whether the project will finish on time and within budget. It includes a prediction/estimate with regards to the probable project completion date and final budget requirements.

NOTE: This summary estimate on completion date and final budget is based on the professional judgment of the appropriate Program Team. There is no definitive approach to developing this section; rather this judgment incorporates common EVMS and schedule probability calculation methods available in the literature. In addition to raw, mathematical calculation results, other factors should be considered including the nature of the contract mechanisms being used (e. g. the percentage of work that is Firm Fixed Price); and the trained and experienced professional judgment of the Program Manager and his/her staff.

7.0 Table of Acronyms and Mathematical Formulas

A table or tables shall be prepared and presented that lists the all the acronyms used in the preparation of this report and all the mathematical formulas, excepting WBS roll-ups, used in calculating EVMS parameters for this report. At a minimum, the lexicon and acronyms used as well as the mathematical formulas used shall match the lexicon, acronyms, and mathematical formulas used in the version of OMB Circular A-11 that is valid as of the date the report is prepared.

8.0 Detailed Tables of Current EVMS Parameters

Tables shall be prepared and presented that list the cumulative EVMS parameters (captured and calculated) for each summary level of the WBS (including WBS levels 4, 3, 2, and 1). One table shall be for the whole EVMS Baseline. The second table shall be for the portions of the EVMS Baseline that are not related to value measured using a Level of Effort (LOE) methodology. At a minimum the tables shall each present the captured or calculated values for the following table columns:

- WBS
- Name/Title
- BCWS
- BCWP
- ACWP
- CV
- CPI
- SV
- SPI
- CPI/SPI
- Baseline BAC
- EAC1
- EAC2
- Estimated BAC
- Baseline Finish Date
- Estimated Finish Date

Preparation of the Electronic EVMS Data Report

An Electronic EVMS Data Report will be prepared and submitted (typically by the 15th of the following month) that supplies input data to the FBI's electronic EVMS data reporting system. The FBI's electronic EVMS reporting system utilizes Métier's WorkLenz. The data contained in the Electronic EVMS Data Report shall be prepared and submitted using Microsoft Project 2003 and Microsoft Excel 2002. Data shall be formatted to match the input requirements of Métier's WorkLenz that is current as of the date of report submittal. Data submitted electronically shall be down to and include WBS level 6 at a minimum.

18.6 Risk Management Plan

The Risk Management Plan describes the contractor processes for risk management planning and budgeting; risk identification, assessment, and analysis; risk response planning; and risk monitoring and control. Organization and content descriptions of the Risk Management Plan are as follows:

Section 1. Introduction

1.1 Purpose
(This section describes the purpose of the risk management plan.)
1.2 Scope
(This sections details the scope of the risk management plan.)
1.3 Assumptions, Constraints, and Policies
(This section describes underlying assumptions, constraints, and government and contractor policies relating to the risk management of the project.)
1.4 Referenced Documents and Standards
(This section contains the following information for any document or standard referenced with the Risk Management Plan: document identifier, title, organization/author, version number, date of publication.)

Section 2. Overview of Risk Management Process

2.1 Overview
2.2 Process and Data Flows
(As part of the description of the risk management process and data flows, this section includes the titular identification of risk management personnel and their roles and responsibilities; frequency of risk management activities; and risk management reporting requirements.)
2.3 Program Management Integration
(This section describes the extent to which project management is integrated into the risk management process.)

Section 3. Organizational Considerations

3.1 SENTINEL Organization
(This section describes how the contractor team is organized and identifies the key members of the risk management processes by name and role. An organizational chart will be included.)
3.2 Program Communications and Responsibilities
(This section describes how communications will be conducted relating to risk management processes, what responsibilities exist in communication, and how timely risk management communications will be maintained in the SENTINEL project.)
3.3 Subcontractor Responsibilities
(This section describes how subcontractors will be integrated into the risk management process, and what their roles and responsibilities will be.)

Section 4. Process Details

4.1 Identifying Risks
(This section describes the process for identifying risks.)
4.2 Analyzing Risks
(This section describes the methods for establishing the probability that a risk will occur and quantifying the impact of occurrence. The section also describes the methods determining the impact of mitigation activities associated with a risk.)
4.3 Planning to Mitigate Risks
(This section describes the methods used in planning to mitigate risks.)
4.4 Tracking and Control of Risks
(This section describes how risks will be tracked, how mitigation efforts will be assessed, and what mechanisms will be used in controlling risk.)
4.5 Summary of Methods, Tools, and Metrics
(This section summarizes the methods, tools, and metrics involved with the risk management processes.)

Section 5. Resources and Schedule of Risk Management Milestones

(This section identifies risk management milestones and describes the associated entrance and exit criteria. The section also identifies the resources to be used in achieving the milestones.)

Section 6. Documentation of Risk Information

(This section describes how risk information will be documented, managed, and accessed.)

Section 7. Methodology Associated with Changes in Scope and Funding

(This section describes the risk management methodology associated managing the project baseline in the event that project scope or funding undergoes significant change.)

18.7 Defect Reports

Government Approved Contractor Format.

18.8 Measurement Plan

Government Approved Contractor Format

Contractor format must address the following elements:

- Measurement Roles, Responsibilities, and Communications
- Description of Program Information Needs
- Definition of each Measurement (detailed)* including Critical Performance Measures (CPMs) as they are established (refer to IT LCMD Appendix H for CPM content requirements)
- Data Collection and Analysis Procedures
- Measurement Evaluation Criteria for each measure
- Data reporting method

Below is a sample measure specification (source: Practical Software and System Measurement) that the contractor can tailor or replace with a suitable substitute. This sample is provided to show the expected level of detail.

Measurement Information Specification

Measure Name

Information Need Description	
Information Need	What the measurement user (e.g., manager or project team member) needs to know in order to make informed decisions.
Information Category	A logical grouping of information needs that are defined in PSM to provide structure for the Information Model. PSM categories include schedule and progress, resources and cost, product size and stability, product quality, process performance, technology effectiveness, and customer satisfaction. Categories are defined in Chapter 2 of the PSM book.

Measurable Concept	
Measurable Concept	An idea for satisfying the information need by defining the entities and their attributes to be measured.

Entities and Attributes	
Relevant Entities	The object that is to be measured. Entities include process or product elements of a project such as project tasks, plans/estimates, resources, and deliverables.
Attributes	The property or characteristic of an entity that is quantified to obtain a base measure.

Base Measure Specification

Base Measures	A base measure is a measure of a single attribute defined by a specified measurement method (e.g., planned number of lines of code, cumulative cost to date). As data is collected, a value is assigned to a base measure.
Measurement Methods	The logical sequence of operations that define the counting rnle to calculate each base measure.
Type of Method	The type of method used to quantify an attribute, either (1) subjective, involving human judgement, or (2) objective, using only established rules to determine numerical values.
Scale	The ordered set of values or categories that are used in the base measure.
Type of Scale	The type of the relationship between values on the scale, eithcr: • Nominal - the measurement values are categorical, as in defects by their type. • Ordinal - the measurement values are rankings, as in assignment of defects to a severity level. • Interval - the measurement values have equal increments for equal quantities of the attribute, such as an additional cyclomatic complexity value for each additional logic path in a software unit. • Ratio - the measurement values have equal increments, beginning at zero, for equal quantities of the attribute, such as size measurement in terms of LOC.
Unit of Measurement	The standardized quantitative amount that will be counted to derive the value of the base measure, such as an hour or a line of code.

Derived Measure Specification	
Derived Measure	A measure that is derived as a function of two or more base measures.
Measurement Function	The formula that is used to calculate the derived measure.

Indicator Specification	
Indicator Description and Sample	A display of one or more measures (base and derived) to support the user in deriving information for analysis and decision making. An indicator is often displayed as a graph or chart. Include a sketch of the indicator.
Analysis Model	A process that applies decision criteria to define the behavior responses to the quantitative results of indicators.
Decision Criteria	A defined set of actions that will be taken in response to achieved quantitative values of the model.
Indicator Interpretation	A description of how the sample indicator (see sample figure in indicator description) was interpreted.

Data Collection Procedure (for each Base Measure) **Complete this seetion for each base measure listed on the previous page.**	
Frequency of Data Collection	How often data is collected.
Responsible Individual	The person who is assigned to collect the data.
Phase or Activity in which Collected	The phase or activity when the data is collected.
Tools Used in Data Collection	List any tools used to collect the data (e.g., source code analyzer).
Verification and Validation	List any V&V tests that will be run to ensure the data is complete and accurate.
Repository for Collected Data	List any tools where data is stored after it is collected (e.g., database).

Data Analysis Procedure (for each Indicator)	
Frequency of Data Reporting	How often data is reported (this may be less frequent than it is collected).
Responsible Individual	The person who is assigned to analyze data and report the results.
Phase or Activity in which Analyzed	The phase or activity when the data is analyzed.
Source of Data for Analysis	List any sources of data for this analysis.
Tools Used in Analysis	List any tools used for analysis (e.g., statistical tools).
Review, Report, or User	Document when results are reviewed and reported, along with the intended user of the results.

Additional Information	
Additional Analysis Guidance	Provide any additional guidance on variations of this measure.
Implementation Considerations	List any process or implementation requirements that are necessary for successful implementation.

18.9 Measurement Report

Government approved contractor format with the following guidance:

Provide monthly metrics reports on the metrics defined in the Measurement Plan. Provide explanations and interpretations of reported metrics data, including deviations from expected or projected values and breaches of thresholds, as well as any corrective actions being undertaken.

18.10 Communications Plan

A template for a Communications Plan is provided at SOW Attachment-5 Communications Plan template. SOW Attachment-5 contains the Government's desired plan content and level of detail. The Communications Plan shall address the topics contained in the attachment.

18.11 Travel Plan

The Travel Plan is a three-month projection of all program-related travel. For each anticipated trip, the Travel Plan contains the following information: SOW task and subtask number, project phase, reason for travel, location, number of people traveling, number of travel days, and estimated cost.

The Travel Plan includes summary-level roll-ups by combined triplet SOW task, SOW Subtask, and Phase (e.g., Task 3, subtask 1, Phase 1); by month; and by the entire three-month period. Summary-level information includes: total number of trips, total number of people-trips (e.g., two people traveling on one trip is 2 people-trips), total number of days of travel, and total anticipated cost. Summary-level quantities for trips crossing month boundaries are prorated by the number of travel days occurring in the given month.

Contractor formatting of the Travel Plan is acceptable.

18.12 EOC Memorandnm of Understanding

The MOU defines the roles and responsibilities of the ITOD's EOC in the performance of SENTINEL operations. The MOU shall define the expected EOC Help Desk Support. The contractor is responsible for all other operations and maintenance activities per the SOW. A sample MOU is appended below containing the expected EOC responsibilities.

Memorandum of Understanding

ITOD Support of SENTINEL Operation

To: (SENTINEL Program Manager) signature_____

From: Kenneth Boyd Signature_____
CC: Julius Brooks, Eileen Short, Hebert Engle, James Loudermilk, John Traxler, Edward Sestak, Gale Scavenghelli, Thomas Paton, Karen Stefflinson, Rick Fergusson
Date:

Re: ITOD's Enterprise Operations Center (EOC) support of SENTINEL operations

---

1. HelpDesk

The EOC's Customer Support (CS) staff will provide help desk assistance via the EOC's 202-324-1500 central support phone number for all problems and requests related to the SENTINEL system.

When the EOC CS staff receives a call from a customer requiring assistance, the CS staff will attempt to resolve the issue using the Call Scripts that were provided by the SENTINEL PMO.

If a user calls to request a SENTINEL password reset, the CS staff will resolve but all other account management requests (new, modified, delete account) will be assigned to the SENTINEL O&M contractor.

If a user calls regarding questions with SENTINEL the EOC CS staff will reference the caller to the SENTINEL website and log a ticket to the SENTINEL O&M contractor for resolution.

If the EOC CS staff cannot resolve the issue and the problems looks to be related to the SENTINEL software or hardware, the problem ticket will be assigned to the SENTINEL O&M contractor for resolution.

SENTINEL hours of Onsite Support: The SENTINEL staff will provide on-site support from 7:30 AM till 4:30 PM EST.

2. Network Service

The EOC's Network staff will not provide any monitoring or troubleshooting support to the SENTINEL network equipment.

3. System/Server Administration

The EOC's System/Server Administration staff will not provide any monitoring or troubleshooting support to the SENTINEL servers.

4. Security Management

The EOC's Security Management staff has no responsibilities for monitoring, account management, security logs, or remote patch management for SENTINEL. The EOC Security staff will provide the SENTINEL team the tested and approved McAfee virus updates via a compact disc.

5. Remote Software

The EOC's Remote Software staff has no responsibilities for software installation or Tier-2 troubleshooting.

6. Other Items to Address

SENTINEL Accounts Management is not a function of SARs and has not been transitioned to the Network Section's System Security Access Unit. All account requests will be facilitated via a problem ticket assigned to the SENTINEL assignment group.

SENTINEL Application support has not been transitioned to the Systems Support Section. All problems, upgrade and maintenance issues are the responsibility of the SENTINEL assignment group.

SENTINEL database support has not been transitioned to the Operation Section's Database Administration Unit. All problems, upgrade and maintenance issues related SENTINEL's databases are the responsibility of the SENTINEL assignment group.

The EOC will not provide 24 x 7 x 365 monitoring support of SENTINEL servers. The SENTINEL O&M contractor will be responsible for all monitoring, problems, upgrades and patch management.

The EOC will not provide 24 x 7 x 365 monitoring support of the SENTINEL network equipment. The SENTINEL O&M contractor will be responsible for all monitoring, problems, upgrades and patch management.

18.13 Risk Assessment (Delivered Twice Monthly)

The Risk Assessment is a report of the total risk exposure of each contractor-identified risk in accordance with the FBI Risk Management Guideline and Standards. The information reported for each active risk includes, at a minimum: unique identifier, title, short description, impact, probability of occurrence, timeframe of concern, and changes in impact, probability of occurrence, and timeframes of concern relative to the preceding report. Tables within the Risk Assessment provide different views of the information by sorting on different elements of information. Specific tables of active risks to be included are:

a. Sort by risk identifier (all active risks in order of increasing identifier)
b. Sort by impact (top *N* active risks in order of decreasing identifier)
c. Sort by probability of occurrence (top *N* active risks in decreasing order of probability)
d. Sort by timeframe (*N* earliest active risks in order of increasing start date)
e. Sort by change in impact (*N* largest changes in decreasing order)
f. Sort by change in probability (*N* largest changes in decreasing order)
g. Sort by change in timeframe (*N* earliest risks whose start dates shift from prior report)

At contract initialization, the value *N* will be specified for each table, although its value may change during the course of the contract to satisfy government needs. The Risk Assessment also summarizes the risks that were closed relative to the preceding report.

Contractor formatting of the Risk Assessment is permitted.

18.14 Integrated Master Schedule (weekly)

Integrated Master Schedule (IMS)	Item Number: **B-2-14**
	Revision #: R01
	Effective Date: 05-28-04

Use

The Integrated Master Schedule (IMS) is an integrated schedule containing the networked, detailed tasks necessary to ensure successful program execution. The IMS shall be used to verify attainability of contract objectives, to evaluate progress toward meeting program objectives, and to integrate the program schedule activities with all related components. The IMS includes significant external interfaces and critical items from suppliers, teammates, or other detailed schedules that depict significant and/or critical elements and Government furnished equipment or information dependencies for the entire contractual effort in a single integrated network.

Interrelationship

The IMS is traceable to the Project Plan, the Work Breakdown Structure (WBS), the Earned Value Management System (EVMS) Baseline and the Statement of Work (SOW). The written document and the associated electronic deliverable are delivered to the Project Manager and the Contracting Officer (if the project is part of a contract)

Preparation information

Preparation of the written IMS Analysis

The IMS Analysis is an assessment of schedule progress to date and includes changes to schedule assumptions, variances to the baseline schedule, causes for the variances, potential impacts, and recommended corrective actions to minimize schedule delays. The analysis shall also identify potential problems and an assessment of the critical path and near-critical paths. The thresholds for reporting significant variances to the baseline schedule are any differences between current schedule date and baseline schedule date for milestones (zero duration) or plus or minus 10% of duration for other tasks/activities. The near critical path is defined as any task/activity with a total float/slack of five work days or less.

Preparation of the Electronic IMS Data Report

1.0 Format

The electronic IMS data shall be reported using Microsoft Project 2003. The electronic IMS data shall be delivered electronically in a Microsoft Project 2003 format, specifically a single *.mpp file or a master *.mpp file accompanied by the linked subproject files in a *.mpp file format.

2.0 Content

The schedule shall contain the contract milestones, accomplishments, and discrete tasks/activities (including planning packages where applicable) from contract award to the completion of the contract. The schedule shall be an integrated, logical network-based schedule that correlates to the WBS, and is vertically and horizontally traceable to the cost/schedule reporting instruments used to address variances such as the EVMS Status Report. It shall contain contractual milestones and descriptions and display summary, intermediate, and detailed schedules, and periodic

analysis of progress to date. It shall include fields and data that enable the user to access the information by product, process, or organizational lines.

2.1 Contract Milestones and Definitions

The schedule shall contain key programmatic events, which define progress and completion for each WBS element, along with the definition for successful completion of the milestone.

2.2 Summary Master Schedule

This schedule shall contain a top-level schedule of key tasks/activities and milestones at the summary levels of the WBS. It shall be an integrated roll up of the intermediate and detailed schedules (see 2.3 and 2.4 below) (vertical integration).

2.3 Intermediate Schedules

These schedules shall be mid-level contract schedules that include key tasks/activities and milestones and all associated accomplishments in the summary master schedule, traceable to the WBS element to display work effort at the intermediate level of summarization. There may be several intermediate schedules that depict varying levels of detail. They shall be integrated roll ups of the detailed schedules (see 2.4 below) (vertical integration).

2.4 Detailed Schedules

These schedules are the lowest level of contract tasks/activities that form the network. The detailed schedules shall contain horizontal and vertical integration, as a minimum, at the work package and planning package level. The detailed schedules shall include all tasks/activities, work packages, and planning packages identified resulting from the Statement of Work (SOW). Every discrete task/activity, work package, and planning package shall be clearly identified and directly related to a control account. Work packages and planning packages shall be individually represented and summarize to or reconcile with the total budget for that control account. If Level of Effort (LOE) control accounts, work packages, or planning packages are included as tasks in the IMS, they shall be clearly identified as such. The detailed tasks/activities, work packages, and planning packages shall be traceable to only one WBS element and only one responsible/performing organizational element, as applicable. The level of detail in the IMS (including number and duration of tasks/activities) shall follow the contractor's EVM process as documented in the EVMS system description, EVMS Baseline program directives, etc. Shorter-term work packages (ideally equal in length to the statusing interval) are preferred because they provide more accurate and reliable measures of work accomplished.

2.4.1 Key Elements of Detailed Schedules

The key elements of the detailed schedules include the following:

1) Task/Activity - An element of work with duration.

2) Milestone - A specific definable accomplishment in the contract network, recognizable at a particular point in time. Milestones have zero duration and do not consume resources.

3) Duration - The length of time estimated (or realized) to accomplish a task/activity.

4) Percent Complete (Schedule) - The proportion of an activity or task that has been completed to time now. This usually involves updating or statusing the activity or task utilizing one of two methods: (1) Update the remaining time to complete (remaining duration) and the scheduling software will then automatically update the schedule percent complete or (2) update the schedule percent complete and allow the scheduling software to calculate the time remaining (remaining duration) to complete. Either method will use the following formula: Percent of Duration Completed = (Actual Duration / Total Duration) X 100.

5) Task/Activity and Milestone Descriptions - These are descriptive titles that are concise, complete, and clearly identify the work effort being accomplished. Abbreviations may be used to shorten the descriptive titles.

6) WBS Codes and Data Dictionary - A list of field definitions and WBS structures. This list shall be provided to the procuring activity.

7) Relationship/Dependency - These identify how predecessor and successor tasks/activities and milestones are logically linked. Relationships, also called network logic, are modeled in four ways:

a) FS (Finish to Start) - A predecessor task/activity or milestone that must finis h before a succeeding task/activity or milestone can start. FS relationships shall be used whenever possible.

b) SS (Start to Start) - A predecessor task/activity or milestone that must start before a succeeding task/activity or milestone can start.

c) FF (Finish to Finish) - A predecessor task/activity or milestone that must finish before a succeeding task/activity or milestone can finish.

d) SF (Start to Finish) - A predecessor task/activity or milestone that must start before a succeeding task/activity or milestone can finish.

8) Total Float/Slack - The amount of time a task/activity or milestone can slip before it delays the contract or project finish date.

9) Free Float/Slack - The amount of time a task/activity or milestone can slip before it delays any of its successor tasks/activities or milestones.

10) Lag - An interval of time that must occur between a predecessor and successor task/activity or milestone. Since negative time is not demonstrable, negative lag is not encouraged. (Note: Lag should not be nsed to manipulate float/slack or constrain schedule.)

11) Early Start (ES) - The earliest start date a task/activity or milestone can begin the precedence relationships. A computer-calculated date.

12) Early Finish (EF) - The earliest finish date a task/activity or milestone can end. A computer-calculated date.

13) Late Start (LS) - The latest start date a task/activity or milestone can start without delaying the contract or project target completion date. A computer-calculated date.

14) Late Finish (LF) - The latest date a task/activity or milestone can finish without delaying the contract or project target completion date. A computer-calculated date.

15) Critical Path - A sequence of discrete tasks/activities in the network that has the longest total duration through the contract or project. Discrete tasks/activitics along the critical path have the

least amount of float/slack. The critical path and near-critical paths are calculated by the scheduling software application. The guidelines for critical path and near-critical path reporting are as follows:

a) Methodology - The IMS software application computes a critical path and near-critical paths based on precedence relationships, lag times, durations, constraints, and status. Artificial constraints and incorrect, incomplete, or overly constrained logic shall be avoided because they can skew the critical path and near-critical paths.

b) Identification - The critical path shall be easily identified.

16) Constraints - Limits applied to network start and finish dates (e.g., "finish no later than"). (Note: Certain types of constraints should be used judiciously because they may impact or distort the network critical path.)

17) Current Schedule - The IMS reflects the current status and forecast. It includes forecasted starts and finishes for all remaining tasks/activities and milestones. Significant variances to the baseline schedule shall be explained in the periodic analysis. Thresholds for reporting shall be specified in the Data Items.

18) Baseline Schedule - Baseline dates in the IMS shall be consistent with the baseline dates in the EVMS Baseline for all work packages, planning packages, and control accounts (if applicable). The guidelines for maintaining the baseline schedule are as follows:

a) Schedule Changes - Changes to the schedule shall be baselined when incorporated into the schedule.

b) Baseline Schedule Changes - Changes to the baseline schedule shall be made in accordance with the Contracting Officer approved EVM process. Any movement of contractual milestones in the baseline schedule shall be derived only from either authorized contract changes or an approved over target schedule.

19) Schedule Progress - The IMS shall reflect actual progress and maintain accurate start and finish dates for all tasks/activities and milestones. The guidelines for reflecting schedule progress are as follows:

a) Actual Start and Finish Dates - Actual start and actual finish dates shall be recorded in the IMS. Actual start and actual finish dates, as recorded, shall not be later than the status date.

b) Progress Line - The progress line depicted in a Gantt chart shall be applied to the current schedule.

20) Retention of Data for Completed Tasks/Activities -Historical performance on completed tasks/activities shall be maintained electronically for analytical use. Historical performance shall be maintained at the time of key program events (Integrated Baseline Review, Critical Design Review, etc.) for all critical tasks/activities. Data to be retained includes logic, actual and baseline durations, actual and baseline start and finish dates, and the three-point estimates that were used before the task/activity started.

21) External Dependencies - The IMS shall identify significant external dependencies that involve a relationship or interface with external organizations, including all Government furnished items (e.g., decisions, facilities, equipment, information, data, etc.). The determination of significant shall be agreed to by the Government and contractor and shall be defined and documented in the Data Items. The required or expected delivery dates shall also be identified in the IMS.

22) Schedule Margin - A management method for accommodating schedule contingencies. It is a designated buffer and shall be identified separately and considered part of the baseline. Schedule

margin is the difference between contractual milestone date(s) and the contractor's planned date(s) of accomplishment.

23) Schedule Risk Assessment - A schedule risk assessment predicts the probability of project completion by contractual dates. Three-point estimates shall be developed for remaining durations of remaining tasks/activities that meet any of the following criteria: (1) critical path tasks/activities, (2) near-critical path tasks/activities (as specified above), and (3) high risk tasks/activities in the program's risk management plan. These estimates include the most likely, best case, and worst case durations. They are used by the contractor to perform a probability analysis of key contract completion dates. The criteria for estimated best and worst case durations shall be applied consistently across the entire schedule and documented in the contractor's sehedule notes and management plans. The guidelines for estimates are as follows:

a) Most Likely Estimate - Schedule durations based on the most likely Estimates.

b) Best/Worst Case Estimates - Best and worst case assumptions shall be disclosed.

The contractor schedule risk assessment shall explain changes to the critical path, margin erosion, and mitigation plans. It shall be incorporated into the
contractor's program risk management process. The initial schedule risk assessment shall be submitted during the Integrated Baseline Review. The risk analysis may be performed within the IMS or within a separate risk tool as appropriate based on the capability of the automated scheduling tool.

24) User Defined Fields - All user defined fields in the IMS shall be identified by providing a mapping of all fields used in the scheduling software application.

25) Reserved Fields - The Government may reserve some fields and/or require the contractor to use certain fields for specific information.

Calendar - The arrangement of normal working days, together with non-working days, such as holidays, as well as special work days (i.e., overtime periods) used to determine dates on which project work will be completed.

18.18 Data Accession List

The contractor shall maintain a current listing of all Program Documentation including title, version, date and location.

18.25 Design Concept Description and Architecture

Use the FBI IT LCMD Appendix H Design Concept Description with the following addition as an appendix to address the Security Architecture as follows:

Appendix A – SENTINEL Security Architecture

1. OVERVIEW AND REQUIREMENTS
1.1 SENTINEL System Architecture Overview
1.2 Security Requirements and Policies
1.3 Philosophy of Protection
1.4 C&A Strategy
1.4.1 Availability
1.4.2 Confidentiality
1.4.3 Data Integrity
1.5 Assumptions and Constraints
2. SENTINEL SYSTEM SECURITY ARCHITECTURE APPROACH
2.1 SENTINEL Security Functions
2.1.1 Identification and Authentication (I&A)
2.1.2 User Authorization
2.1.3 User Account Administration
2.1.4 Filtering and Anomaly Detection
2.1.5 Access Control
2.1.6 Auditing and Audit Reporting
2.2 SENTINEL Security Implementation
2.2.1 Security Server
2.2.2 Directory Server
2.2.3 Discretionary Access Controls
2.3 Data Integrity
2.4 Security Organizational Controls
2.4.1 System Administrator (SYSADMIN)
2.4.2 Configuration Management Manager (CMM)
2.4.3 Information Systems Security Manager (ISSM)
2.4.4 Computer System Security Officer (CSSO)
2.5 Legacy Interfaces
2.6 Communications Networks
2.7 Physical Security

18.36 Service Level Agreement (SLA)

The SLA shall be developed in a Government approved contractor specified format. The SLA shall contain the following elements:

Duration - Specify when the agreement begins and expires.

Roles and responsibilities-Define the roles and responsibilities of the customer, the Government service level manager, and the service provider.

Descriptions of service- Include specific descriptions of the services to be provided (a service catalog), including applications, infrastructure, and other business functions.

Service standards – Define the performance targets to be met. Reference sources where available (e.g., SOW, SRS). Define operating hours for each service and associated levels of service.

Sample Measurements and Performance Targets

Measurement	Definition	Performance Target
SLA Table from SOW Section 15		
SENTINEL system availability		Per the SRS
SENTINEL system response time		Per the SRS
SENTINEL capacity management		Per the SRS
SENTINEL data backup		Per the SRS, PUG
SENTINEL personnel response time		1 hour
SENTINEL periodic maintenance time		Not to exceed two hours per week
SENTINEL disaster recovery times		Per the contingency plan
SENTINEL user account set up time		
Trouble ticket response times		Per the EOC handbook
Trouble ticket resolution times		Per the EOC handbook
Alert deadlines (low medium, high, critical)		Per the EOC handbook

Evaluation Methods and Reports -Establish objective means to determine how well the system and the O&M team are delivering to the service standards. Establish the reports, source of data and frequency of reporting.

Policies, Procedures, Standards – Reference the policies, procedures, and standards to be employed in support of the services covered under this SLA.

Incentives and Penaltics- Establish the incentives with achieving or exceeding target levels. Establish penalties associated with not meeting targets.

18.39 Data Migration Plan

Identify the scope of the data migration efforts (e.g., what data elements to be migrated, whether open transactional data will migrate, the amount of historical data to convert, error correction plan). Describe the data migration process, to include the roles and responsibilities of participants and the identity of the process owner. Identify potential risks, verification strategies, migration dependencies, and volume considerations. Provide specific and measurable criteria for migration success. Provide a data migration schedule, by Phase, that includes when the data will be captured, converted, verified for correctness and completeness, and available for use in the new system software.

By project Phase, identify for each file of migrating data:

- Location of migrating data
- Legacy software that accessed migrating data
- Quantity of migrated data
- Form of data
- Conversions required to be compatible with new system
- Error correction requirements
- New software that will access the migrated data
- Expected size of migrated data
- Expected location of migrated data
- Means of verifying correctness and completeness of data migration

The contractor formatting of the Data Migration Plan is acceptable.

18.40 EOC Operational Support Requirements Doeument of New Systems

Federal Bureau of Investigation
Information Resources Division
Customer Relations Management Section
Enterprise Operations Center Unit

EOC OPERATIONAL SUPPORT REQUIREMENTS DOCUMENT FOR NEW SYSTEMS

Program/System Name:

Brief Description of System:

FBI Program Manager:	**Phone:**
Security/C&A POC:	**Phone:**
ISSM:	**Phone:**
ISSO:	**Phone:**
Sponsor:	**Phone:**
Technical Lead:	**Phone:**
	Pager:

Operational Support Plan

- **Implementation schedule**

_____

_____

_____

- **Division/Section/Unit(s)**that provides Tier2 Support (Touch Labor)

  _____

  Hours Supported:

  _____

- **Division/Section/Unit(s)** that provides Tier3 Support (Application and/or Engineering)

  _____

  Hours Supported:

  _____

- **Division/Section/Unit(s)** that provides Access Support

  _____

  Hours Supported:

  _____

EOC Standard Operating Procedures (Attach Docs)

- **Call Scripts**: Yes / No
- **Frequently Asked Questions & Answers**: Yes / No

EOC Transition Plan

- **For EOC Tier 1 HelpDesk**
- **For EOC Tier 1 System Administration**
- **For EOC Tier 1 Network Services**
- **For EOC Tier 1 Security Management**

Additional EOC Support Resources:

- **Costs Associated with Resources**
  $ _____

EOC Training

- **For EOC Tier 1 HelpDesk**
- **For IRD Tier 1 System Administration**
- **For EOC Tier 1 Network Services**
- **For EOC Tier 1 Security Management**

Hardware Associated with new System?

- Yes / No
- If yes, explain and complete below.

Property Number Serial No Device Type CostCode

EOC Server/Mainframe Monitoring Required?

- Yes / No
- If yes, explain.

- EMS Tools Used

- New EMS Tools Needed
  Yes / No
  If yes, explain.

Software Associated with new System?

- Yes / No
- If yes, list software below

Software Name	Platform (e.g. Mainframe, Server, Desktop)

Database Associated with new System?

- Yes / No
- If yes, list software below

Database Name	Platform (e.g. Mainframe, Server, Desktop)

Operational Level Agreements (OLA's)

(Response times between EOC and IRD/Contract Support Staff)

Service Level Agreements (SLA's)

(Providing resolution times to the customer by Subcategory)

Critical Page List

Last, First, MI	Pager	Position

Additional EOC Support Costs

- **Resources**
  $ _____
- **Software**
  $ _____
- **Hardware**
  $ _____

- **Categories/Subcategories/Assignment Groups**

CATEGORY - SUBCATEGORY - DIV/SECTION/UNIT - DESCRIPTION

Application_____
Application_____
Application_____
Application_____
Software_____
Software_____
Software_____
Software_____
Hardware_____
Hardware_____
Hardware_____
Hardware_____
Network_____
Network_____
Network_____
Network_____
Security_____
Security_____
Security_____
Security_____
User_____
User_____
User_____
User_____

ServiceCenter Access Needed?

Yes / No

ServiceCenter Access Procedures.

Each person that requires access to ServiceCenter will require a SAR (http://itod.fbinet.fbi/sc/sar/sarhqdivisionpoc.pdf) to be opened for FBINet Mainframe access first (http://itod.fbinet.fbi/sc/scaccess.htm). The process is below.

To Request:

- New or modified access to one (or many) of the ServiceCenter Application's modules ...
- Removal of access to the ServiceCenter Application ...
- Accessor ID (ACID) login changes to the ServiceCenter Application ...
- Email address changes to the ServiceCenter application.

You Must Have:

- FBINET accessor ID issued by Systems Security Access Unit . If you do not have an ACID, a SAR will need to be submitted.(http://itod.fbinet.fbi/sc/sar/sarhqdivisionpoc.pdf)
- A current record in the BPMS system. (If non-FBI with an FBINET ACID, enter a record via PCUS. (http://30.100.100.8:8180/contact/servlet/Contact)

Follow these steps:

1. Fill out and print the ServiceCenter Access Request Form. If you select OTHER as the "user's job type" on the basic access request form, also complete the Amended ServiceCenter Access Request Form.
2. Complete the mandatory fields and the specific type of access you are requesting.
3. Have your supervisor sign the form to validate request.
4. Fax completed form(s) to (202) 324-6720, Attention: IIAU-SCPT.

A Service Problem ticket will be opened and assigned to D4/SDS/IISCU-SCPT for processing. A member of the ServiceCenter Program Team (SCPT) will notify the requester once the access has been granted.

ISSUES/CONCERNS/COMMENTS

18.41 DCU04 Request for Data Center Access

DCU04 Rev. 11/14/04

Request For Data Center Access

Program Name: _____ Date:

Program Manager: _____ Room:

Division / Section / Unit: _____ Ext: _____

Name	Company / Agency	Clearance Level	Access Begin Date	Access End Date	Access Type	Escort Authority (Yes/No)

(Note: When bringing equipment into the Data Center, a completed DCU05 form "Data Center Equipment Installation Requirements" is required before the equipment may enter Data Center space.)

Instructions

Name: Name of person(s) needing access
Company/Agency: Employing company/agency
Clearance Level: Clearance granted by FBI - include SCI access if applicable
Access Begin Date: Requested date to begin access to the Data Center
Access End Date: Date to end access to the Data Center (note: access must be updated semi-annually)
Access Type: Unrestricted (Only FBI Personnel Assigned In Data Center), Unescorted (must have TS/SCI), or Escorted
Escort Authority: Request to allow this person to escort (must be an FBI employee with TS/SCI)

_____
(Requesting Unit Chief) Date

_____
(DCU Chief) Date

18.42 DCU05 Request for Data Center Equipment Installation

DCU05 11/03

REQUEST FOR DATA CENTER EQUIPMENT INSTALLATION

Program Name: _____ Date: _____

Program Manager: _____ Room: _____

Division / Section / Unit: _____ Ext. _____

DESCRIPTION OF EQUIPMENT TO BE INSTALLED AND SPACE/POWER COOLING/CONNECTIVITY REQUIRED:

Examples:

c(2105) Server	1 5	13-23-65/F1111111 2R85V21/F1323900	IBM(Z900) via Ficon FBINET via Gigabit Ethernet	L6-30R(2) Nema 5-15(6)	60 15	DUAL DUAL Or SINGLE	47 KBTU 2400 BTU	3"x9" 4"x12"

Item Make/Model	Qty	Serial# and Property#	Connects to: attach wiring diagram	Power Recept Type/#	Power Amps	UPS Connect	Hea BTU

Notes: Attach equipment diagram with physical size and space needed to service equipment.

_____
(Requesting Unit Chief) Date

_____
(DCU Chief) Date

18.53 Technical Manual (Non-Commercial HW ouly)

Use the guidelines established in FBI IT LCMD Appendix H with the following additional guidance: Commercial manuals shall be delivered and are considered suitable substitutes for the technical manual. Technical manuals are only required in the event a commercial manual is not available, modifications are made to off the shelf hardware, or custom hardware is developed.

18.65 Product (CSCI's)

This is the physical software.

18.66 Logical Data Model

The contractor shall develop a logical data model using the Government model as point of departure. The content shall include, at a minimum, the same type of information contained in the Government model. The data model shall be exportable to the Government data modeling tool (ERWIN).

18.68 O&M Procedures

The contractor shall prepare supplemental procedures to assist the TIER 1 Call Center, operations, etc., as required to support, streamline and enhance operations and maintenance. Contractor format is acceptable.

18.69 O&M Transition Plan

1. Scope. This section shall be divided into the following paragraphs.

1.1 Identification. This paragraph shall contain a full identification of the system to which this document applies, including, as applicable, identification number(s), title(s), abbreviation(s), version number(s), and release number(s).

1.2 System Overview. This paragraph shall briefly state the purpose of the system to which this document applies. It shall describe the general nature of the system; and summarize operation and maintenance activities; and list other relevant documents.

1.3 Document Overview. This paragraph shall summarize the purpose and contents of this document and shall describe any security or privacy considerations associated with its use.

2. Referenced Documents. This section shall list the number, title, revision, and date of all documents referenced in this report. This section shall also identify the source for all documents not available through normal Government stocking activities.

3. Transition Plan. This section shall be divided into the following paragraphs to provide an overview of the Transition Plan. To include all activities, facilities, documentation, Government assistance, and incumbent contractor assistance needed to successfully transition from the current operations and maintenance support contract to the operations and maintenance contract resulting from this solicitation.

3.1 Overall process to accomplish Transition Plan objectives. This paragraph(s) shall, at a minimum, address the following:

a. Introduction: Introduces this Transition Plan and discusses the scope, objective, and summary of the transition process.

b. Documentation: Lists the Transition Plan guidance documents and information documents. Presents a documentation tree for the documents needed to implement the transition process.

c. Transition Overview: Presents an executive overview of the transition process and provides a Transition Overview Diagram for easy reference.

d. Transition Management: Describes the method for managing the transition process. Describes the method and measures for measuring the transition process success.

e. Transition Resources: Describes the resources needed to implement the transition process. Describes roles and responsibilities in completing the transition process.

f. Transition Tasks: Describes the tasks to be accomplished to complete the transition process. Included in the tasks shall be the activities needed to seamlessly integrate contracted services into the CJIS System-of-Services.

g. Task Dependencies: Describes the task dependencies and establishes a master schedule.

h. Assumptions and Constraints: Describes assumptions and constraints used within the transition process.

i Transition Cost Estimate, Not-to-Exceed Transition Price, and basis for those estimates.

3.2 Recommended Improvements. This paragraph shall provide any recommended improvements in the operation and maintenance activities that support transition. A discussion of each recommendation and its impact on the system may be provided. If no recommended improvements are provided, this paragraph shall state "None."

4. Notes. This section shall contain any general information that aids in understanding this document (e.g., background information, glossary, rationale). This section shall include an alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document and a list of any terms and definitions needed to understand this document.

18.70 SENTINEL Stakeholder and Organizational Risk Assessment

A template for the SENTINEL Stakeholder and Organizational Risk Assessment is provided at SOW Attachment-7 Communications and Strategy Action Plan template. SOW Attachment-7 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.71 Organization Impact Assessment (OIA)

A template for the Organizational Impact Assessment is provided at SOW Attachment-8 Organizational Impact Assessment template. SOW Attachment-8 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.76 Agendas, Briefings, Meeting Minutes

Content shall be at the contractor's discretion and judgment to meet the purpose of the supported conference/meeting/review.

18.77 Workforce Transformation Strategy and Plan

A template for the Workforce Transformation Strategy and Plan is provided at SOW Attachment-9 Workforce Transformation Strategy and Plan template. SOW Attachment-9 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.78 Integrated Master Plan

The Integrated Master Plan shall conform to the IMP content guidelines contained in AFMC Pamphlet 63-5, Integrated Master Plan and Schedule Guide 11 November 2004. The IMP shall include key process descriptions.

18.79 Training Strategy and Plan

A template for the Training Strategy and Plan is provided at SOW Attachment-6 Training Strategy and Plan template. SOW Attachment-6 contains the Government's desired plan content and level of detail. The plan shall address the topics contained in the attachment.

18.80 Training Administration Report

A template for a Training Administration Report is provided at SOW Attachment-10 Training Administration Report template. The attachment contains the Government desired report content. The report shall address the topics contained in the attachment.

18.81 Delivery Acceptance Report

FBS Offeror to propose.

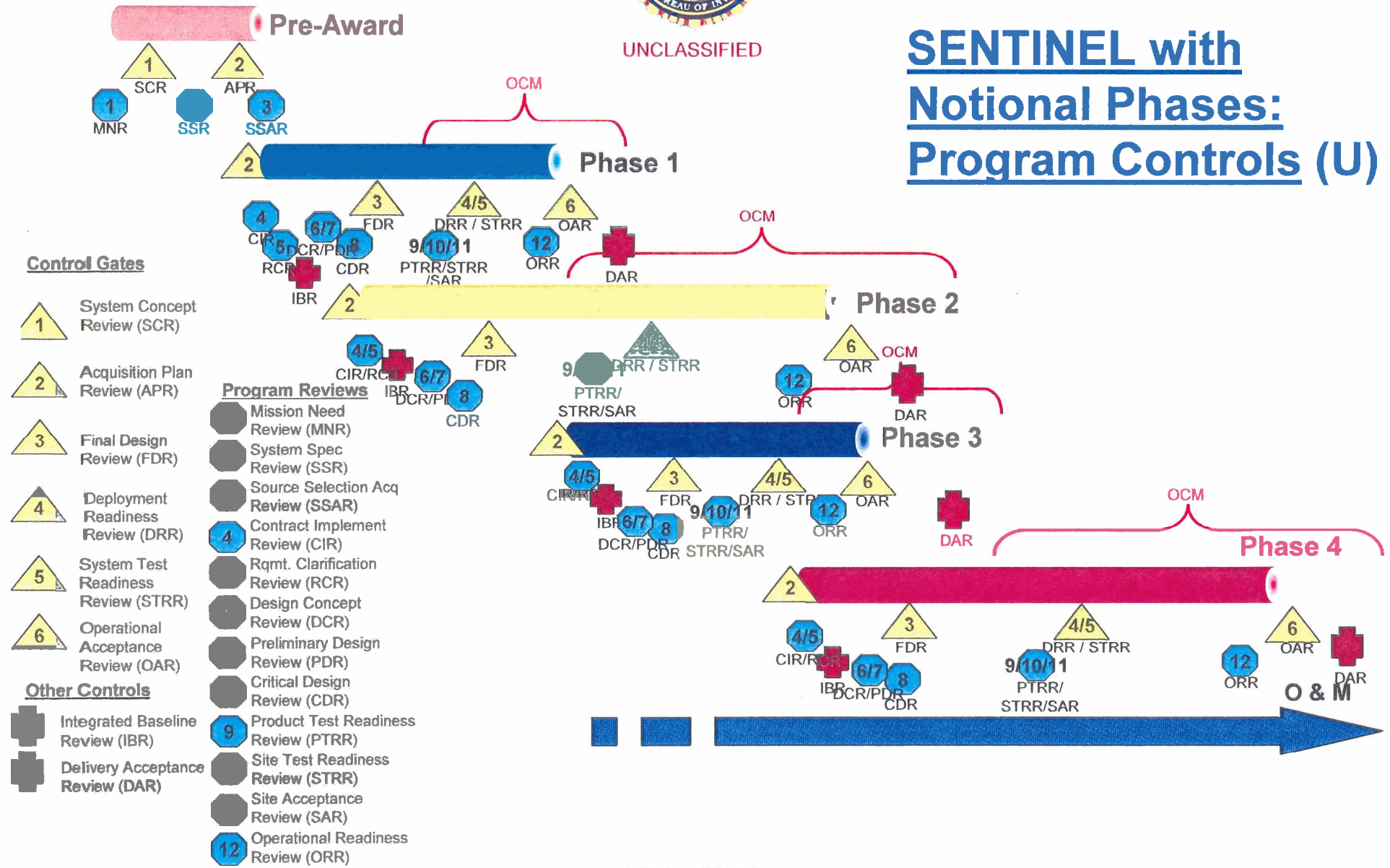
ENCLOSURE B

QUESTION 11d

SENTINEL MILESTONES

UNCLASSIFIED

SENTINEL with Notional Phases: Program Controls (U)



UNCLASSIFIED

ENCLOSURE C

QUESTION 22b

NATIONAL RESPONSE PLAN

1. **Terrorism Incident Law Enforcement and Investigation Annex**

2. **Nuclear/Radiological Incident Annex**

3. **Biological Incident Annex**

ENCLOSURE C

1. Terrorism Incident Law Enforcement and Investigation Annex

Terrorism Incident Law Enforcement and Investigation Annex

Coordinating Agency:

Department of Justice/Federal Bureau of Investigation

Cooperating Agencies:

Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of State
Environmental Protection Agency

Introduction

Purpose

The purpose of this annex is to facilitate an effective Federal law enforcement and investigative response to all threats or acts of terrorism within the United States, regardless of whether they are deemed credible and/or whether they escalate to an Incident of National Significance. To accomplish this, the annex establishes a structure for a systematic, coordinated, unified, timely, and effective national law enforcement and investigative response to threats or acts of terrorism within the United States.

Scope

This annex is a strategic document that:

- Provides planning guidance and outlines operational concepts for the Federal law enforcement and investigative response to a threatened or actual terrorist incident within the United States; and
- Acknowledges and outlines the unique nature of each threat or incident, the capabilities and responsibilities of the local jurisdictions, and the law enforcement and investigative activities necessary to prevent or mitigate a specific threat or incident.

Policies

The United States regards terrorism as a potential threat to national security, as well as a violent criminal act, and applies all appropriate means to combat this danger. In doing so, the United States vigorously pursues efforts to deter and preempt these crimes and to apprehend and prosecute directly, or assist other governments in prosecuting, individuals who perpetrate or plan terrorist attacks.

To ensure the policies established in applicable Presidential directives are implemented in a coordinated manner, this annex provides overall guidance to Federal, State, local, and tribal agencies concerning the Federal Government's law enforcement and investigative response to potential or actual terrorist threats or incidents that occur in the United States, particularly those involving weapons of mass destruction (WMD), or chemical, biological, radiological, nuclear, or high-explosive (CBRNE) material.

Federal Agencies

The law enforcement and investigative response to a terrorist threat or incident within the United States is a highly coordinated, multiagency State, local, tribal, and Federal responsibility. In support of this mission, the following Federal agencies have primary responsibility for certain aspects of the overall law enforcement and investigative response:

- Department of Defense (DOD)
- Department of Energy (DOE)
- Department of Health and Human Services (HHS)
- Department of Homeland Security (DHS)
- Department of Justice/Federal Bureau of Investigation (FBI)
- Environmental Protection Agency (EPA)

According to HSPD-5, "The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 and other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with U.S. law and with activities of other Federal departments and agencies to protect our national security, to assisting the Attorney General to identify the perpetrators and bring them to justice. The Attorney General and the Secretary shall establish appropriate relationships and mechanisms for cooperation and coordination between their two departments."

Although not formally designated under this annex, other Federal departments and agencies may have authorities, resources, capabilities, or expertise required to support terrorism-related law enforcement and investigation operations. Agencies may be requested to participate in Federal planning and response operations, and may be requested to designate liaison officers and provide other support as required.

Deployment/Employment Priorities

In addition to the priorities identified in the National Response Plan (NRP) Base Plan, the law enforcement and investigative response to terrorist threats or incidents is based on the following priorities:

- Preserving life or minimizing risk to health; which constitutes the first priority of operations.
- Preventing a threatened act from being carried out or an existing terrorist act from being expanded or aggravated.
- Locating, accessing, rendering safe, controlling, containing, recovering, or disposing of a WMD that has not yet functioned, and disposing of CBRNE material in coordination with appropriate departments and agencies (e.g., DOD, DOE, EPA).
- Apprehending and successfully prosecuting perpetrators of terrorist threats or incidents.

Planning Assumptions and Considerations

In addition to the planning assumptions and considerations identified in the NRP Base Plan, the law enforcement and investigative response to terrorist threats or incidents, particularly those involving WMD and CBRNE material, are based on the following assumptions and considerations:

- A terrorist threat or incident may occur at any time of day with little or no warning, may involve single or multiple geographic areas, and may result in mass casualties.
- The suspected or actual involvement of terrorists adds a complicating dimension to incident management.
- The response to a threat or actual incident involves FBI law enforcement and investigative activity as an integrated element.

- In the case of a threat, there may be no incident site, and no external consequences, and, therefore, there may be no need for establishment of traditional Incident Command System (ICS) elements such as an Incident Command Post (ICP) or a Joint Field Office (JFO).

- An act of terrorism, particularly an act directed against a large population center within the United States involving nuclear, radiological, biological, or chemical materials, will have major consequences that can overwhelm the capabilities of many local, State, and/or tribal governments to respond and may seriously challenge existing Federal response capabilities.

- In the case of a biological attack, the effect may be temporally and geographically dispersed, with no determined or defined "incident site." Response operations may be conducted over a multijurisdictional, multistate region.

- A biological attack employing a contagious agent may require quarantine by Federal, State, local, and tribal health officials to contain the disease outbreak.

- If appropriate personal protective equipment and capabilities are not available and the area is contaminated with CBRNE or other hazardous materials, it is possible that response actions into a contaminated area may be delayed until the material has dissipated to a level that is safe for emergency response personnel to operate or until appropriate personal protective equipment and capabilities arrive, whichever is sooner.

Situation

The complexity, scope, and potential consequences of a terrorist threat or incident require that there be a rapid and decisive capability to resolve the situation. The resolution to an act of terrorism demands an extraordinary level of coordination of law enforcement, criminal investigation, protective activities, emergency management functions, and technical expertise across all levels of government. The incident may affect a single location or multiple locations, each of which may be an incident scene, a hazardous scene, and/or a crime scene simultaneously.

Concept of Operations

Command and Control

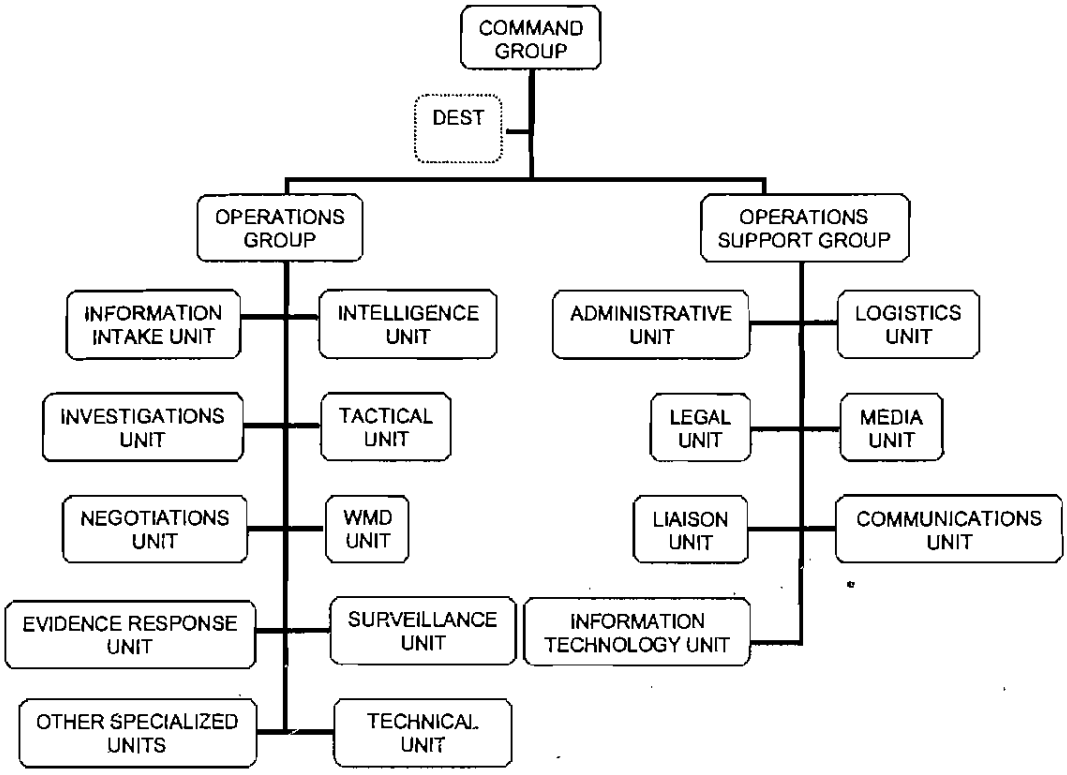
The FBI is the lead agency for criminal investigations of terrorist acts or terrorist threats and intelligence collection activities within the United States. Investigative and intelligence activities are managed by the FBI from an FBI command post or Joint Operations Center (JOC). The command post or JOC coordinates the necessary Federal law enforcement assets required to respond to and resolve the threat or incident with State, local, and tribal law enforcement agencies.

The FBI Special Agent in Charge (SAC) of the local Field Office establishes a command post to manage the threat based upon a graduated and flexible response. This command post structure generally consists of three functional groups: Command, Operations, and Operations Support, and is designed to accommodate participation of other agencies, as appropriate (see Figure 1).

When the threat or incident exceeds the capabilities and resources of the local FBI Field Office, the SAC can request additional assistance from regional and national assets to augment existing capabilities. In a terrorist threat or incident that may involve a WMD or CBRNE material, the traditional FBI command post will transition to a JOC, which may temporarily incorporate a fourth functional entity, the Consequence Management Group (see Figure 2), in the absence of an activated JFO.

When, in the determination of the Secretary of Homeland Security, in coordination with the Attorney General, the incident becomes an Incident of National Significance and a JFO is established, the JOC becomes a section of the JFO and the FBI SAC becomes the Senior Federal Law Enforcement Official (SFLEO) in the JFO Coordination Group. In this situation, the JOC Consequence Management Group is incorporated into the appropriate components of the JFO (see NRP Base Plan, Figure 4 and Figure 7).

FIGURE 1. FBI command post



The JOC structure may also be used to coordinate law enforcement, investigative, and intelligence activities for the numerous threats or incidents that occur each year that do not escalate to Incidents of National Significance.

Joint Operations Center

- The JOC is an interagency command and eontrol center for managing multiagency preparation for, and the law enforcement and investigative response to, a credible terrorist threat or incident. Similar to the Area Command concept within the ICS, the JOC also may be established to coordinate and organize multiple agencies and jurisdictions during critical incidents or special events. Following the basic principles established in the National Incident Management System (NIMS), the JOC is modular and scalable and may be tailored to meet the specific operational requirements needed to manage the threat, incident, or special event.

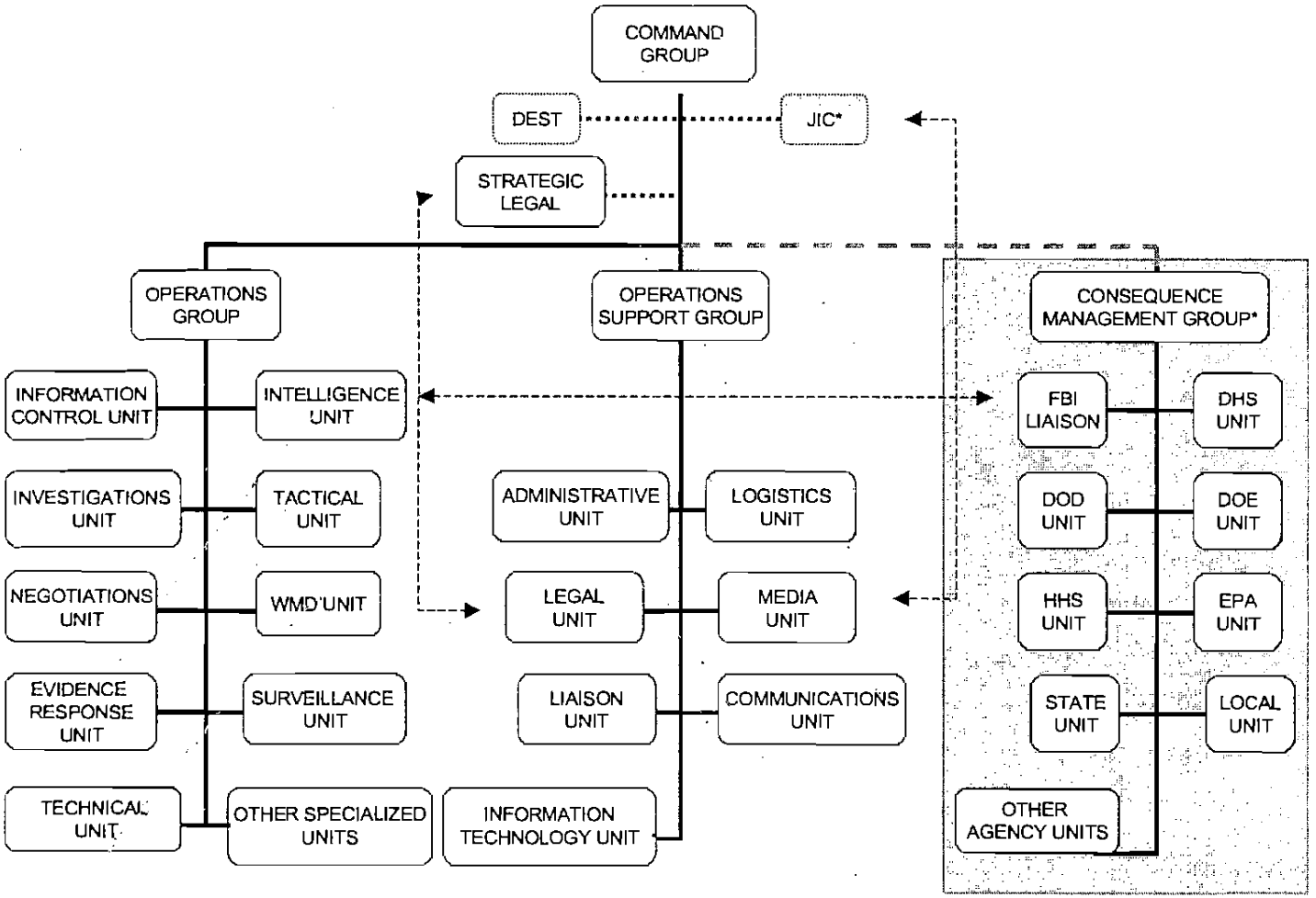
- A JOC may be established and staffed in a pre-incident, pre-emptive role in support of a significant special event. This "watch mode" allows for rapid expansion to full operations if a critical incident occurs during the special event. The JOC is a strategic management tool that effectively coordinates law enforcement investigative, intelligence, and operational activities at multiple sites from a single location. The JOC may be the only management structure related to a threat, critical incident, or special event, or it may integrate into other management structures in accordance with the NRP.

- Law enforcement public safety functions, such as proactive patrol and traffic control, historically are managed through the Operations Section of the ICS. Criminal investigation and the collection, analysis, and dissemination of intelligence are sensitive law enforcement operations that requirc a secure environment and well-defined organizational management structure. The JOC is designed to coordinate this specialized law enforcement investigative and intelligence activity. It provides mechanisms for controlling access to and dissemination of sensitive or classified information. Management of crisis information and intelligence is recognized under the NIMS as a sixth functional area within ICS. The structure of the JOC supports this functional area and enhances the overall management of critical incidents and special events.

- The NIMS provides the framework within which the ICS and JOC structures operate for a unified approach to domestic incident management.

- The JOC is composed of four main groups: the Command Group, the Operations Group, the Operations Support Group, and the Consequence Management Group.

FIGURE 2. Joint Operations Center



* While the Operations Group and Operations Support Group remain components of the JOC when it is incorporated into the JFO, the JIC and Consequence Management Group will be merged into the appropriate JFO staff components, if established.

Command Group

- The Command Group of the JOC provides recommendations and advice to the FBI SAC regarding the development and implementation of strategic decisions to resolve the situation. It is responsible for approving the deployment and employment of law enforcement investigative and intelligence resources. The Command Group maintains its advisory role to the FBI SAC when the JOC becomes a section of the JFO for an Incident of National Significance. When a JFO is established in this situation, the FBI SAC becomes the SFLEO in the JFO Coordination Group. The Assistant SAC or an alternate senior FBI official leads the JOC Command Group once the SAC has transitioned to the JFO.

- The FBI representatives in the Command Group include the SAC, the Assistant SAC, and an executive-officer position known as the Crisis Management Coordinator (CMC). The SAC of the FBI Field Office in which the incident occurs is responsible for developing the overall strategy for managing Federal investigative law enforcement activities at the critical incident or special event and coordinating the implementation of that strategy with other agency decisionmakers and FBI Headquarters. The FBI SAC also is responsible for coordinating Federal law enforcement activities with other Federal incident management personnel during domestic critical incidents and special events. The CMC ensures that the strategy of the SAC is communicated to everyone in the JOC and that the JOC is staffed and equipped to effectively implement the strategy of the SAC. The CMC also ensures that information flows efficiently within the JOC and between the JOC and other command and control centers.

- The JOC Command Group includes senior officials with decisionmaking authority from local, State, and Federal agencies, as appropriate, based upon the circumstances of the threat or incident. Consistent with the Unified Command concept, law enforcement investigative and intelligence strategies, tactics, and priorities are determined jointly within the JOC Command Group. Federal law enforcement investigative, intelligence, and operational decisions are made cooperatively to the extent possible, but the authority to make these decisions rests ultimately with the FBI SAC.

- Three specialized teams provide guidance and expertise directly to the Command Group. These teams are the Strategic Legal Team, the Joint Information Center Team, and the Domestic Emergency Support Team.

  - The Strategic Legal Team is composed of legal counsel from the FBI, U.S. Attorney's Office, and the District or State's Attorney's Office. This team provides legal guidance to the Command Group concerning the strategies under consideration for resolution of the crisis.

  - The Joint Information Center (JIC) Team is integrated into the JFO when established. It is composed of the public affairs (media) officers from the participating local, State, and Federal public safety agencies. It manages information released to the public through a coordinated, unified approach. A separate media unit within the JOC Operations Support Group provides FBI-specific guidance and expertise to the FBI SAC and coordinates with the JIC to ensure the media strategy is consistent with the overall investigative strategy.

  - The Domestic Emergency Support Team (DEST) is a specialized interagency team composed of subject-matter experts from the FBI, the DHS/Emergency Preparedness and Response/Federal Emergency Management Agency (DHS/EPR/FEMA), DOD, DOE, HHS, and EPA. It provides guidance to the FBI SAC concerning WMD threats and actual incidents.

Operations Group

- The Operations Group handles all investigative, intelligence, and operational functions related to the threat, critical incident, or special event.

- Each unit within the Operations Group provides expertise in a specific functional area that is important in the overall resolution of the incident.

- The units within the Operations Group are scalable and modular, and may be tailored to the specific threat, critical incident, or special event.

- The Operations Group normally consists of the Information Intake unit (formerly referred to as the Control unit), the Intelligence unit, the Investigations unit, and Field Operations units.

Information Intake (or Control)

- Information Intake is the central point for receiving all information that comes into the JOC. The purpose of Information Intake is to ensure that telephone calls, e-mail messages, fax reports, and other incoming information are assessed for relevance to the threat, critical incident, or special event. The information is checked to determine if it has been previously reported. It is prioritized and entered into the information management system. Through this filtering mechanism the Information Intake unit ensures that only current and relevant information is disseminated to the JOC.

- The Information Intake Coordinator is responsible for providing guidance and direction to all personnel within the Information Intake unit and coordinating the activities of the unit with all other units within the JOC. Personnel within the Information Intake unit are responsible for receiving incoming information, processing new information, routing followup information appropriately, and implementing procedures for tracking evidentiary material that is introduced into the command post.

Intelligence

- The Intelligence unit manages the collection, analysis, archiving, and dissemination of relevant and valid investigative and strategic intelligence. It fuses historical intelligence from a variety of sources with new intelligence specific to the threat, critical incident, or special event. The Intelligence unit also disseminates intelligence products and situation reports to all JOC units, FBI Headquarters Strategic Information and Operations Center (SIOC), and the JFO Coordination Group. This information is shared with the DHS Homeland Security Operations Center (HSOC), the National Counterterrorism Center (NCTC), and, as appropriate, other government agencies, consistent with operational security considerations.

- The Intelligence unit usually is divided into teams based on functional responsibility. Teams manage intelligence related to the crisis site or target, build intelligence portfolios and databases on significant elements related to the investigation (subjects, vehicles, and organizations), analyze and identify trends in activities related to the investigation (predictive and strategic intelligence), conduct liaison with outside members of the Intelligence Community, and prepare periodic briefings and reports concerning the status of the crisis or investigation. The Intelligence unit is responsible for collecting and reviewing all intelligence related to the threat, crisis, or special event to enable the SAC to further develop and refine strategic objectives.

Investigations

- The Investigations unit provides oversight and direction to all investigative activity related to the threat, critical incident, or special event. The Investigations unit implements the strategy of the SAC by directing the collection and management of investigative information. It is composed of investigative personnel from the agencies with specific jurisdiction or authority for investigating crimes related to the threat, critical incident, or special event. The Investigations Unit Coordinator is usually an FBI Supervisor who has responsibility for investigating the most significant substantive law violation.

- Teams within the Investigations unit review all incoming information to determine investigative value. The Investigations unit assigns, tracks, and reviews all investigative leads and documents the investigation in the appropriate case file(s). The case agents or primary investigators within the Investigations unit manage all evidence and information, and prepare it for court presentation, if appropriate. The case agents or primary investigators are assisted by analytical personnel to ensure that all investigative information is pursued to its logical conclusion. A Records Check Team within the Investigations unit reviews case files and databases to ensure that all items of investigative value are identified and evaluated. The Investigations unit is responsible for collecting and reviewing all reports of investigative activity to enable the SAC to further develop and refine strategic objectives.

Field Operations

- The Field Operations units are based upon the specific needs of the threat, critical incident, or special event. The personnel staffing these units are subject-matter experts in a number of specialized skill areas. Field Operations unit coordinators are responsible for ensuring the activity of the specialized units is consistent with and in support of the strategy of the SAC.

- Field Operations units may include representatives of tactical, negotiations, WMD/CBRNE, evidence response, surveillance, technical, or any other specialized unit deployed to the crisis site(s) or staged in readiness. The mission of these units is to provide the SAC with current information and specialized assistance in dealing with the threat, critical incident, or special event. Information is communicated between the JOC and the crisis site(s) through the Field Operations unit representatives in the JOC. This ensures that decisionmakers both in the JOC and in the forward areas maintain full situational awareness. The Field Operations units coordinate their activities within the JOC to ensure each is aware of the impact of their activities on the other field units.

- Local, State, and Federal law enforcement specialty units assigned to assist with field operations during the threat, incident, or special event coordinate their activities with the appropriate FBI Field Operations units through the JOC. Federal Government mission-specific units are designated to help the FBI maintain their respective chains of command and coordinate their activities through representation in the JOC. The JOC manages the activities of the specialized units at a strategic level. Activities at the individual or "tactical" level are managed at the crisis site(s) through forward command structures such as the Tactical Operations Center, Negotiations Operations Center, and Evidence Response Team Operations Center.

Operations Support Group

- The Operations Support Group units designated within the JOC are based upon the specific needs of the threat, critical incident, or special event. The personnel who staff these units are subject-matter experts in a number of specialized areas. Operations Support Group unit coordinators are responsible for ensuring the activity of their units is consistent with and in support of the strategy of the SAC.

- Operations Support Group units can include administrative, logistics, legal, media, liaison, communications, and information management. The mission of these units is to support the investigative, intelligence, and operational functions of the JOC.

- The Administrative and Logistics units have responsibilities that are similar to the Finance and Logistics Sections in ICS. However, they are tasked with managing only the activities related to the law enforcement investigative, intelligence, and operational functions; they do not manage the administrative and logistics functions associated with the overall incident.

- The Legal and Media units support the investigative and intelligence operations of the JOC through the preparation of specific legal processes and management of media affairs. These units focus on specific objectives related to the investigation such as search warrants and press releases, and not the strategic overall objectives handled by the Strategic Legal Team and JIC that are attached to the Command Group.

- The Liaison unit is composed of representatives from outside agencies who assist the FBI with resolution of the threat, critical incident, or special event. The Liaison unit may include agencies without clear authority or jurisdiction over the threat, critical incident, or special event if they have a potential investigative interest. For example, law enforcement agencies that border affected jurisdictions may be represented in the JOC to maintain situational awareness of potential threats. Additional Liaison unit representatives may include fire department personnel, utility company workers, or engineering specialists.

- The Communications unit handles radio and telephone communications to support JOC operations. The Communications unit establishes communications networks within the JOC. It also establishes networks to facilitate timely and reliable information-sharing between the JOC and other command and control centers.

- The Information Technology unit is responsible for the JOC computer system operation within each unit and between units. Information technology specialists and facilitators assigned to this unit are responsible for ensuring the uninterrupted operation of the information management system used during JOC operations.

Consequence Management Group

- The JOC Consequence Management Group consists of representatives of agencies that provide consequence-focused expertise in support of law enforcement activities. The JOC does not manage consequence functions; rather, it ensures that law enforcement activities with emergency management implications are communicated and coordinated to appropriate personnel in a complete and timely manner.

- A DHS representative coordinates the actions of the JOC Consequence Management Group, and expedites activation of a Federal incident management response should it become necessary. FBI and DHS representatives screen threat/incident intelligence for the Consequence Management Group. Representatives of the JOC Consequence Management Group monitor the law enforcement criminal investigation and may provide advice regarding decisions that impact the general public or critical infrastructure. This integration provides continuity should a Federal incident management response become necessary.

- Agencies comprising the Consequence Management Group may also have personnel assigned to other units within the JOC structure. Depending on the nature of the incident and required assets, additional teams assigned to support the FBI may be included under Other Specialized Units.

- Should the threat of a terrorist incident become imminent, the JOC Consequence Management Group may forward recommendations to the RRCC Director to initiate limited pre-deployment of assets under the Stafford Act.

- Requests for DOD assistance for law enforcement and criminal investigation during the incident come from the Attorney General to the Secretary of Defense through the DOD Executive Secretary. Once the Secretary approves the request, the order is transmitted either directly to the unit involved or through the Chairman of the Joint Chiefs of Staff. The FBI SAC informs the Principal Federal Official (PFO), if one has been designated, when requesting this additional assistance.

- The Consequence Management Group is established when a JOC is necessary but a JFO has not yet been activated, or the event has not reached the level of being considered an Incident of National Significance.

- Representatives in this group may move to appropriate positions in other sections of the JFO when one is established.

The Response

- Receipt of a terrorist threat may be through any source or medium and may be articulated or developed through intelligence sources. It is the responsibility of all local, State, and Federal agencies and departments to notify the FBI when such a threat is received. As explained below, the FBI evaluates the credibility of the terrorist threat and notifies the HSOC, NCTC, and other departments and agencies, as appropriate.

- Upon receipt of a threat of terrorism within the United States, the FBI conducts a formal threat credibility assessment in support of operations with assistance from select interagency experts. For a WMD or CBRNE threat, this assessment includes three perspectives:

  - Technical Feasibility: An assessment of the capacity of the threatening individual or organization to obtain or produce the material at issue;

  - Operational Practicability: An assessment of the feasibility of delivering or employing the material in the manner threatened; and

  - Behavioral Resolve: A psychological assessment of the likelihood that the subject(s) will carry out the threat, including a review of any written or verbal statement by the subject(s).

- A threat assessment is conducted to determine whether the potential threat is credible, and confirm whether WMD or CBRNE materials are involved in the developing terrorist incident. Intelligence varies with each threat and impacts the level of the Federal response. If the threat is credible, the situation requires the tailoring of response actions to use Federal resources needed to anticipate, prevent, and/or resolve the situation. The Federal response focuses on law enforcement/investigative actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat. In addition, contingency planning focuses on the response to potential consequences and the pre-positioning of tailored resources, as required. The threat increases in significance when the presence of a CBRNE device or WMD capable of causing a significant destructive event, prior to actual injury or loss, is confirmed or when intelligence and circumstances indicate a high probability that a device exists. In this case, the threat has developed into a WMD or CBRNE terrorist situation requiring an immediate process to identify, acquire, and plan the use of Federal resources to augment State, local, and tribal authorities in lessening or averting the potential consequence of terrorist use or employment of WMD or CBRNE material. It should be noted that a threat assessment would also be conducted if an incident occurs without warning. In this case, the assessment is focused on criminal intent, the extent of the threat, and the likelihood of secondary devices or locations.

- The FBI manages a Terrorist Threat Warning System to ensure that vital information regarding terrorism reaches those in the U.S. counterterrorism and law enforcement community responsible for countering terrorist threats. This information is coordinated with DHS and the NCTC, and is transmitted via secure teletype. Each message transmitted under this system is an alert, an advisory, or an assessment—an alert if the terrorist threat is credible and specific, an advisory if the threat is credible but general in both timing and target, or an assessment to impart facts and/or threat analysis concerning terrorism.

- Upon determination of a credible threat, FBI Headquarters activates its SIOC to coordinate and manage the national-level support to a terrorism incident. At this level, the SIOC generally mirrors the JOC structure operating in the field. The SIOC is staffed by liaison officers from other Federal agencies who coordinate with and provide assistance to the FBI. The SIOC serves as the focal point for law enforcement operations and maintains direct connectivity with the HSOC. The HSOC is notified immediately by the SIOC once a threat has been determined to be credible. In turn, this notification may result in activation of NRP components in coordination with the FBI.

- The FBI leads the criminal investigation related to the incident, and the SIOC is the focal point for all intelligence related to the investigative law enforcement response to the incident. Consistent with the NRP, affected Federal agencies operate headquarters-level emergency operations centers, as necessary. FBI Headquarters initiates appropriate liaison with other Federal agencies to activate their operations centers and provide liaison officers to the SIOC. In addition, FBI Headquarters initiates communications with the SAC of the responsible Field Office, apprising him/her of possible courses of action and discussing deployment of the DEST. The FBI SAC establishes initial operational priorities based upon the specific circumstances of the threat or incident. This information is then forwarded to FBI Headquarters to coordinate identification and deployment of appropriate resources.

- The JOC is established by the FBI under the operational control of the FBI SAC, and acts as the focal point for the field coordination of criminal investigation, law enforcement, and intelligence activities related to the threat or incident. When a PFO is designated for a terrorism incident, the FBI SAC provides full and prompt cooperation, resources, and support to the PFO, as appropriate and consistent with applicable authorities. The PFO (or an initial PFO designated by the Secretary of Homeland Security) may elect to use the JOC as an initial operating facility for strategic management and identification of State, local, and tribal requirements and priorities, and coordination of the Federal response. The FBI SAC coordinates with the PFO, including providing incident information to the PFO as requested, coordinating the public communications strategy with the PFO, and approving Federal interagency communieations for release to the public through the PFO. It is recognized, however, that in some cases it may be necessary for the FBI SAC to respond directly to media/public inquiries on investigative operations and matters affecting law enforcement operations, particularly during the early stages of the emergency response.

- The local FBI Field Office activates a Crisis Management Team to establish the JOC in the affected area, possibly collocated with an existing emergency operations facility. In locating the JOC, consideration is given to the possibility that the facility may have to accommodate other Federal incident management field aetivities including the JFO, the JIC, and other supporting teams. Additionally, the JOC is augmented by outside agencies, including representatives from the DEST (if deployed), who provide interagency technical expertise as well as interagency continuity during the transition from an FBI command post structure to the JOC structure.

- Based upon a credible threat assessment and a request by the SAC, the FBI Director and DHS Under Secretary for Emergency Preparedness and Response, in consultation with tbe Attorney General and Secretary of Homeland Security, may request authorization through the National Security Council to deploy the DEST to assist the SAC in mitigating the crisis situation. The DEST is a rapidly deployable, interagency team responsible for providing expert advice and support concerning the Federal Government's capabilities in resolving the terrorist threat or incident. This includes law enforcement, criminal investigation, and emergency management assistance, technical and scientific advice, and contingency planning guidance tailored to situations involving chemical, biological, or nuclear/radiological weapons.

- Upon arrival at the FBI command post or JOC, the DEST may act as a stand-alone advisory team to the SAC providing recommended courses of action. Although it would be unusual, the DEST may be tasked to deploy before a JOC is established. The DEST may handle some of the specialized interagency functions of the JOC until the JOC is fully staffed. The DEST emergency management component merges into the Consequence Management Group in the JOC structure.

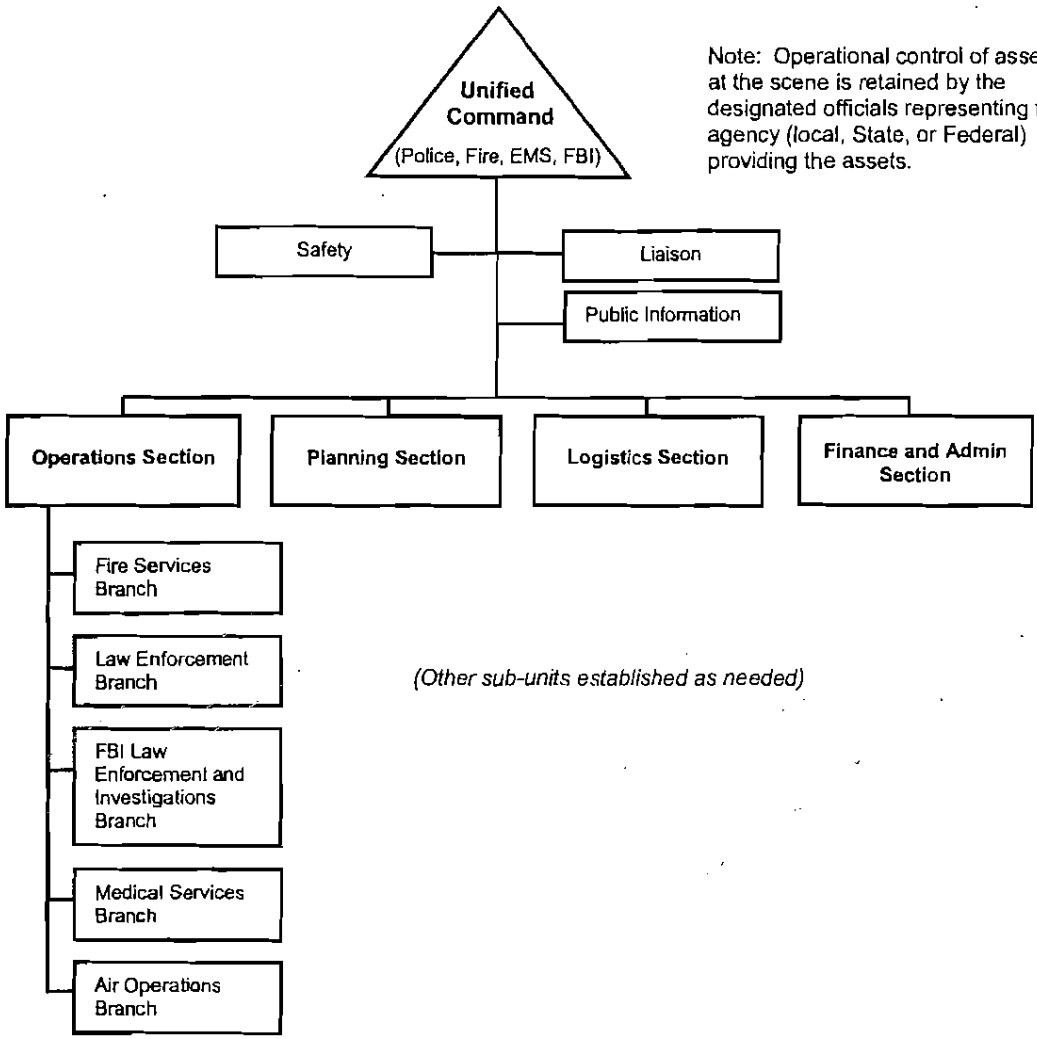
- Prior to an actual WMD or CBRNE incident, law enforcement, intelligence, and investigative activities generally have priority. When an incident results in the use of WMD or CBRNE material, rescue and life-safety activities generally bave priority. Activities may overlap and/or run concurrently during the incident management, and are dependent on the threat and/or the strategies for responding to the incident.

- Upon determination that applicable law enforeement/intelligence goals and objectives are met and no further immediate threat exists, the FBI SAC may deactivate the JOC and order a return to routine law enforcement/investigative operations in accordance with pre-event protocols.

- When an incident occurs and an ICP is established on-scene, FBI personnel integrate into the ICP to enhance the ability of the FBI to carry out its mandated mission (see Figure 3). Three specific positions within an ICP are provided. The first FBI Special Agent (SA) or Joint Terrorism Task Force (JTTF) member responding receives an initial briefing from the Incident Commander or his/her designee and works closely with the Incident Commander as a member of the Unified Command. The FBI representative then informs the local Field Office of the current situation and, if necessary, requests additional assets. When a more senior FBI SA arrives on the scene, he/she assumes the role of the FBI representative in the Unified Command.

- The first arriving SA or JTTF member moves to the Operations Section as the Deputy Chief of Operations. This position is responsible for managing the deployment and coordination of Federal law enforcement and investigative assets in support of the Incident Action Plan. Additionally, an FBI SA assumes the position of Deputy Chief of Planning within the ICP. This position permits the FBI SA to remain updated on the situation and serve as a conduit for requests for additional law enforcement and investigative assets. The Agent also inputs Federal objectives into the developing incident action plan and performs other duties as appropriate. Also, FBI assets form a unit in the Operations Section. Throughout the incident, the actions and activities of the Unified Command at the incident scene and the Command Group of the JOC (and the JFO Coordination Group if established) are continuously and completely coordinated throughout the incident.

FIGURE 3. On-scene coordination



ENCLOSURE C

2. Nuclear/Radiological Incident Annex

Nuclear/Radiological Incident Annex

Coordinating Agencies:

Department of Defense
Department of Energy
Department of Homeland Security
Environmental Protection Agency
National Aeronautics and Space Administration
Nuclear Regulatory Commission

Cooperating Agencies:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of Veterans Affairs
Environmental Protection Agency
General Services Administration
Nuclear Regulatory Commission
American Red Cross

Introduction

Purpose

The Nuclear/Radiological Incident Annex provides an organized and integrated capability for a timely, coordinated response by Federal agencies to terrorist incidents involving nuclear or radioactive materials (Incidents of National Significance), and accidents or incidents involving such material that may or may not rise to the level of an Incident of National Significance. The Department of Homeland Security (DHS) is responsible for overall coordination of all actual and potential Incidents of National Significance, including terrorist incidents involving nuclear materials.

This annex describes how the coordinating agencies and cooperating agencies support DHS's overall coordination of the response to a nuclear/radiological Incident of National Significance. In addition, this annex describes how the coordinating agencies lead the response to incidents of lesser severity. [1]

The actions described in this annex may be implemented: (1) concurrently with, and as an integral part of, the National Response Plan (NRP) for all nuclear/radiological incidents or accidents considered to be Incidents of National Significance; or (2) independently for all other nuclear/radiological accidents or incidents considered to be below the threshold of an Incident of National Significance and, therefore, not requiring overall Federal coordination by DHS.

[1] Nuclear/radiological incidents of "lesser severity" are considered below the threshold of an Incident of National Significance, as determined by DHS, and vary from lost radiography sources or discovery of orphan radiological sources to incidents/emergencies at nuclear power plants below the classification of General Emergency, as defined by the cognizant regulatory agency (e.g., Department of Energy (DOE) or Nuclear Regulatory Commission (NRC)).

Scope

This annex applies to nuclear/radiological incidents, including sabotage and terrorist incidents, involving the release or potential release of radioactive material that poses an actual or perceived hazard to public health, safety, national security, and/or the environment. This includes terrorist use of radiological dispersal devices (RDDs) or improvised nuclear devices (INDs) as well as reactor plant accidents (commercial or weapons production facilities), lost radioactive material sources, transportation accidents involving nuclear/ radioactive material, and foreign accidents involving nuclear or radioactive material.

The level of Federal response to a specific incident is based on numerous factors, including the ability of State, local, and tribal officials to respond; the type and/or amount of radioactive material involved; the extent of the impact or potential impact on the public and environment; and the size of the affected area.

In situations where threat analysis includes indications that a terrorist incident involving radiological materials could occur, actions are coordinated in accordance with the pre-incident prevention protocols set forth in the NRP Base Plan.

This annex:

- Provides planning guidance and outlines operational concepts for the Federal response to any nuclear/radiological incident, including a terrorist incident, that has actual, potential, or perceived radiological consequences within the United States or its territories, possessions, or territorial waters, and that requires a response by the Federal Government. This includes both Incidents of National Significance and incidents of lesser severity;
- Acknowledges the unique nature of a variety of nuclear/radiological incidents and the responsibilities of Federal, State, local, and tribal governments to respond to them;
- Describes Federal policies and planning considerations on which this annex and Federal agency-specific nuclear/radiological response plans are based;
- Specifies the roles and responsibilities of Federal agencies for preventing, preparing for, responding to, and recovering from nuclear/radiological incidents;
- Includes guidelines for notification, coordination, and leadership of Federal activities, and coordination of public information, congressional relations, and international activities; and
- Provides protocols for coordinating Federal Government capabilities to respond to radiological incidents. These capabilities include, but are not limited to:
  - The Interagency Modeling and Atmospheric Assessment Center (IMAAC), which is responsible for production, coordination, and dissemination of consequence predictions for an airborne hazardous material release;
  - The Federal Radiological Monitoring and Assessment Center (FRMAC), established at or near the scene of an incident to coordinate radiological assessment and monitoring; and
  - The Advisory Team for Environment, Food, and Health (known as "the Advisory Team"), which provides expert recommendations on protective action guidance.

  More information on these capabilities is included in subsequent sections of this annex.

Policies

- DHS coordinates the overall Federal Government response to radiological Incidents of National Significance in accordance with Homeland Security Presidential Directive-5 and the NRP. In the NRP Base Plan, Figure 4, Structure for NRP Coordination: Terrorist Incident, illustrates the organizational framework that DHS utilizes to respond to terrorist incidents. In the NRP Base Plan, Figure 5, Structure for NRP Coordination: Federal-to-Federal Support, illustrates the organizational framework that DHS utilizes to respond to nonterrorist Incidents of National Significance.

- The NRP supersedes the Federal Radiological Emergency Response Plan, dated May 1, 1996.

- The concept of operations described in this annex recognizes and addresses the unique challenges associated with and the need for specialized technical expertise/actions when responding to RDD/IND incidents with potentially catastrophic consequences.

- DHS, as the overall incident manager for Incidents of National Significance, is supported by coordinating agencies and cooperating agencies. Coordinating agencies have specific nuclear/radiological technical expertise and assets for responding to the unique characteristics of these types of incidents. Coordinating agencies facilitate the nuclear/ radiological aspects of the response in support of DHS. For any given incident, the coordinating agency is the Federal agency that owns, has custody of, authorizes, regulates, or is otherwise designated responsibility for the nuclear/ radioactive material, facility, or activity involved in the incident. The coordinating agency is represented in the Joint Field Office (JFO) Coordination Group, the Interagency Incident Management Group (IIMG), and the Homeland Security Operations Center (HSOC). The coordinating agency is also represented in other response centers and entities, as appropriate for the specific incident.

- Coordinating agencies are also responsible for leading the Federal response to nuclear/ radiological incidents of lesser severity (those incidents that do not reach the level of an Incident of National Significance).

- Coordinating agencies may use the structure of the NRP to carry out their response duties, or any other structure consistent with the National Incident Management System (NIMS) capable of providing the required support to the affected State, local, or tribal government.

- Cooperating agencies include other Federal agencies that provide technical and resource support to DHS and the coordinating agencies. These agencies are represented in the IIMG, the HSOC, and other response centers and entities, as appropriate for the specific incident. They may or may not be represented in the JFO Coordination Group.

- DHS/Emergency Preparedness and Response/Federal Emergency Management Agency (DHS/EPR/FEMA) is responsible for maintaining and updating this annex. DHS/EPR/FEMA accomplishes this responsibility through the Federal Radiological Preparedness Coordinating Committee (FRPCC).

- The Attorney General, generally acting through the Federal Bureau of Investigation (FBI), has lead responsibility for criminal investigations of terrorist acts or terrorist threats and for coordinating activities of other members of the law enforcement community to detect, prevent, preempt, investigate, and disrupt terrorist attacks against the United States, including incidents involving nuclear/radioactive materials, in accordance with the following:

  - The Atomic Energy Act directs the FBI to investigate all alleged or suspected criminal violations of the act. Additionally, the FBI legally is responsible for locating any illegally diverted nuclear weapon, device, or material and for restoring nuclear facilities to their rightful custodians. In view of its unique responsibilities under the Atomic Energy Act (amended by the Energy Reorganization Act), the FBI has concluded formal agreements with the coordinating agencies that provide for interface, coordination, and technical support for the FBI's law enforcement and criminal investigative efforts.

  - Generally, for nuclear facilities and materials in transit, the designated coordinating agency and cooperating agencies perform the functions delineated in this annex and provide technical support and assistance to the FBI in the performance of its law enforcement and criminal investigative mission. Those agencies supporting the FBI additionally coordinate and manage the technical portion of the response and activate/request assistance under this annex for measures to protect the public health and safety. In all cases, the

FBI manages and directs the law enforcement and intelligence aspects of the response, while coordinating its activities with appropriate Federal, State, local, and tribal governments within the framework of this annex, and/or as provided for in established interagency agreements or plans. Further details regarding the FBI response are outlined in the Terrorism Incident Law Enforcement and Investigation Annex.

- All Federal nuclear/radiological assistance capabilities outlined in this annex are available to support the Federal response to a terrorist threat, whether or not the threat develops into an actual incident.

- When the concept of operations in this annex is implemented, existing interagency plans that address nuclear/radiological incident management are incorporated as supporting plans and/or operational supplements (e.g., the National Oil and Hazardous Substances Pollution Contingency Plan (NCP)).

- This annex does not create any new authorities nor change any existing ones.

- Nothing in this annex alters or impedes the ability of Federal departments and agencies to carry out their specific authorities and perform their responsibilities under law.

- Some Federal agencies are authorized to respond directly to certain incidents affecting public health and safety. In these cases, procedures outlined in this annex may be used to coordinate the delivery of Federal resources to State, local, and tribal governments, and to coordinate assistance among Federal agencies for incidents that can be managed without the need for DHS coordination (i.e., incidents below the threshold of an Incident of National Significance).

- The owner/operator of a nuclear/radiological facility primarily is responsible for mitigating the consequences of an incident, providing notification and appropriate protective action recommendations to State, local, and/or tribal government officials, and minimizing the radiological hazard to the public. The owner/operator has primary responsibility for actions within the facility boundary and may also have responsibilities for response and recovery activities outside the facility boundary under applicable legal obligations (e.g., contractual; licensee; Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)).

- State, local, and tribal governments primarily are responsible for determining and implementing measures to protect life, property, and the environment in those areas outside the facility boundary or incident location. This does not, however, relieve nuclear/radiological facility or material owners/operators from any applicable legal obligations.

- State, local, and tribal governments and owners/operators of nuclear/radiological facilities or activities may request assistance directly from DHS, other Federal agencies, and/or State governments with which they have preexisting arrangements or relationships.

- Response to nuclear/radiological incidents affecting land owned by the Federal Government is coordinated with the agency responsible for managing that land to ensure that incident management activities are consistent with Federal statutes governing use and occupancy. In the case of tribal lands, tribal governments have a special relationship with the U.S. Government, and Federal, State, and local governments may have limited or no authority on specific tribal reservations. Further guidance is provided in the Tribal Relations Support Annex.

- Participating Federal agencies may take appropriate independent emergency actions within the limits of their own statutory authority to protect the public, mitigate immediate hazards, and gather information concerning the emergency to avoid delay.

- Departments and agencies are not reimbursed for activities conducted under their own authorities unless other agreements or reimbursement mechanisms exist (e.g., Stafford Act, Federal-to-Federal assistance).

- Federal coordination centers and agency teams provide their own logistical support consistent with agreed upon interagency execution plans. State, local, and tribal governments are encouraged to coordinate their efforts with the Federal effort, but maintain their own logistical support, consistent with applicable authorities and requirements.

- For radiological incidents involving a nuclear weapon, special nuclear material, and/or classified components, the agency with custody of the material (the Department of Defense (DOD), the Department of Energy (DOE), or the National Aeronautics and Space Administration (NASA)) may establish a National Defense Area (NDA) or National Security Area (NSA). NDAs and NSAs are established to safeguard classified information and/or restricted data, or equipment and material, and place non-Federal lands under Federal control for the duration of the incident. In the event radioactive contamination occurs, Federal officials coordinate with State and local officials to ensure appropriate public health and safety actions are taken outside the NDA or NSA.

Planning Assumptions

- Radiological incidents may not be immediately recognized as such until the radioactive material is detected or the effects of radiation exposure are manifested in the population.

- An act of radiological terrorism, particularly an act directed against a large population center within the United States, will have major consequences that can overwhelm the capabilities of many local, State, and/or tribal governments to respond and may seriously challenge existing Federal response capabilities.

- A radiological incident may include chemical or biological contaminants, which may require concurrent implementation of the NCP or other Federal plans and procedures.

- An incident involving the potential release of radioactivity may require implementation of protective measures.

- An expeditious Federal response is required to mitigate the consequences of the nuclear/radiological incident. Radiological Incidents of National Significance that result in significant impacts likely will trigger implementation of the NRP Catastrophic Incident Annex and Catastrophic Incident Supplement.

- The Federal Government response to radiological terrorist threats/incidents also includes the following assumptions:

  - If appropriate personal protective equipment and capabilities are not available and the area is contaminated by radioactive material, response actions in a contaminated area may be delayed until the material has dissipated to a safe level for emergency response personnel or until appropriate personal protective equipment and capabilities arrive, whichever is sooner;

  - The response to a radiological threat or actual incident requires an integrated Federal Government response;

  - In the case of a radiological terrorist attack, the effect may be temporarily and geographically dispersed, requiring response operations to be conducted over a multijurisdictional, multistate region; and

  - A radiological terrorist incident may affect a single location, or multiple locations, each of which may require an incident response and a crime scene investigation simultaneously.

Concept of Operations

General

This concept of operations is applicable to potential and actual radiological Incidents of National Significance requiring DHS coordination and other radiological incidents of lesser severity, utilizing the protocols delineated in this annex. For other radiological incidents of lesser severity, other Federal response plans (i.e., the NCP and/or agency-specific radiological incident response plans) may also be utilized, as appropriate.

Hazard-Specific Planning and Preparedness

Headquarters

- The Federal Radiological Policy Coordinating Committee (FRPCC) provides a national-level forum for the development and coordination of radiological prevention and preparedness policies and procedures. It also provides policy guidance for Federal radiological incident management activities in support of State, local and tribal government radiological emergency planning and preparedness activities. The FRPCC is an interagency body consisting of the coordinating and cooperating agencies discussed in this annex, chaired by DHS/EPR/FEMA. The FRPCC establishes subcommittees, as necessary.

- The FRPCC also coordinates research-study efforts of its member agencies related to State, local and tribal government radiological emergency preparedness to ensure minimum duplication and maximum benefits to State and local governments. The FRPCC coordinates planning and validating requirements of each agency, reviewing integration requirements and incorporating agency-specific plans, procedures, and equipment into the response system.

Regional: Regional Assistance Committees (RACs) in the DHS/EPR/FEMA regions serve as the primary coordinating structure at the Federal regional level. RAC membership mirrors that of the FRPCC, and RACs are chaired by a DHS/EPR/FEMA regional representative. Additionally, State emergency management agencies send representatives to RAC meetings and participate in regional exercise and training activities. The RACs provide a forum for information-sharing, consultation, and coordination of Federal regional awareness, prevention, preparedness, response, and recovery activities. The RACs also assist in providing technical assistance to State and local governments and evaluating radiological plans and exercises.

Coordinating Agencies and Cooperating Agencies

During a response to an Incident of National Significance, coordinating agencies and cooperating agencies provide technical expertise, specialized equipment, and personnel in support of DHS, which is responsible for overall coordination of incident management activities. Coordinating agencies have primary responsibilities for Federal activities related to the nuclear/radiological aspects of the incident.

The coordinating agency is that Federal agency which owns, has custody of, authorizes, regulates, or is otherwise deemed responsible for the radiological facility or activity involved in the incident. The following paragraphs identify the coordinating agency for a variety of radiological incidents. For example, the Nuclear Regulatory Commission (NRC) is the coordinating agency for incidents involving nuclear facilities licensed by the NRC; DOE is the coordinating agency for incidents involving the transportation of radioactive materials shipped by or for DOE. Table 1 identifies the coordinating agency for a variety of radiological incidents.

Radiological Terrorism Incidents:

- The coordinating agency provides technical support to DHS, which has overall responsibility for domestic incident management, and to the FBI, which has the lead responsibility for criminal investigations of terrorist acts or terrorist threats. The FBI also is responsible for coordinating activities of other members of the law enforcement community to detect, prevent, preempt, investigate, and disrupt terrorist attacks against the United States, including incidents involving nuclear/radioactive materials (e.g. RDD/IND incidents).

TABLE 1. Coordinating agencies

Note: DHS is responsible for the overall coordination of incident management activities for all nuclear or radiological Incidents of National Significance, including those involving terrorism.

Type of Incident	Coordinating Agency
a. Radiological terrorism incidents (e.g., RDD/IND or radiological exposure device):	
(1) Material or facilities owned or operated by DOD or DOE	(1) DOD or DOE
(2) Material or facilities licensed by NRC or Agreement State	(2) NRC
(3) All others	(3) DOE
b. Nuclear facilities:	
(1) Owned or operated by DOD or DOE	(1) DOD or DOE
(2) Licensed by NRC or Agreement State	(2) NRC
(3) Not licensed, owned, or operated by a Federal agency or an Agreement State, or currently or formerly licensed facilities for which the owner/operator is not financially viable or is otherwise unable to respond	(3) EPA
c. Transportation of radioactive materials:	
(1) Materials shipped by or for DOD or DOE	(1) DOD or DOE
(2) Shipment of NRC or Agreement State-licensed materials	(2) NRC
(3) Shipment of materials in certain areas of the coastal zone that are not licensed or owned by a Federal agency or Agreement State (see USCG list of responsibilities for further explanation of "certain areas")	(3) DHS/USCG
(4) All others	(4) EPA
d. Space vehicles containing radioactive materials:	
(1) Managed by NASA or DOD	(1) NASA or DOD
(2) Not managed by DOD or NASA impacting certain areas of the coastal zone	(2) DHS/USCG
(3) All others	(3) EPA
e. Foreign, unknown or unlicensed material:	
(1) Incidents involving foreign or unknown sources of radioactive material in certain areas of the coastal zone	(1) DHS/USCG
(2) All others	(2) EPA
f. Nuclear weapon accident/incident (based on custody at time of event)	DOD or DOE
Other types of incidents not otherwise addressed above	DHS designates

- For radiological terrorism incidents involving materials or facilities owned or operated by DOD or DOE, DOD or DOE is the coordinating agency, as appropriate.

- For radiological terrorism incidents involving materials or facilities licensed by the NRC or Agreement States, the NRC is the coordinating agency.

- For all other radiological terrorist incidents, DOE is the coordinating agency. The coordinating agency role transitions from DOE to the Environmental Protection Agency (EPA) for environmental cleanup and site restoration at a mutually agreeable time, and after consultation with State, local, and tribal governments, the cooperating agencies, and the JFO Coordination Group.

Nuclear Facilities:

- The NRC is the coordinating agency for incidents that occur at fixed facilities or activities licensed by the NRC or an Agreement State. These include, but are not limited to, commercial nuclear power plants, fuel cycle facilities, DOE-owned gaseous diffusion facilities operating under NRC regulatory oversight, independent spent fuel storage installations, radiopharmaceutical manufacturers, and research reactors.

- DOD or DOE is the coordinating agency for incidents that occur at facilities or vessels under their jurisdiction, custody, or control. These incidents may involve reactor operations, nuclear material, weapons production, radioactive material from nuclear weapons or munitions, or other radiological activities.

- EPA is the coordinating agency for incidents that occur at facilities not licensed, owned, or operated by a Federal agency or an Agreement State, or currently or formerly licensed facilities for which the owner/operator is not financially viable or is otherwise unable to respond.

Transportation of Radioactive Materials:

- Either DOD or DOE is the coordinating agency for transportation incidents involving DOD or DOE materials, depending on which of these agencies has custody of the material at the time of the incident.

- The NRC is the coordinating agency for transportation incidents that involve radiological material licensed by the NRC or an Agreement State.

- DHS/U.S. Coast Guard (DHS/USCG) is the coordinating agency for the shipment of materials in certain areas of the coastal zone that are not licensed or owned by a Federal agency or Agreement State.

- EPA is the coordinating agency for shipment of materials in other areas of the coastal zone and in the inland zone that are not licensed or owned by a Federal agency or an Agreement State.

Space Vehicles Containing Radioactive Materials:

- NASA is the coordinating agency for missions involving NASA space vehicles or joint space vehicles with significant NASA involvement. DOD is the coordinating agency for missions involving DOD space vehicles or joint space vehicles with significant DOD involvement. A joint venture is an activity in which the U.S. Government has provided extensive design/financial input; has provided and maintains ownership of instruments, spacecraft, or the launch vehicle; or is intimately involved in mission operations. A joint venture is not created by simply selling or supplying material to a foreign country for use in its spacecraft.

- DHS/USCG is the coordinating agency for space vehicles not managed by DOD or NASA impacting certain areas of the coastal zone.

- EPA is the coordinating agency for all other space vehicle incidents involving radioactive material.

Foreign, Unknown, or Unlicensed Material: EPA or DHS/USCG is the coordinating agency depending on the location of the incident. DHS/USCG is the coordinating agency for incidents involving foreign or unknown sources of radioactive material in certain areas of the coastal zone. EPA is the coordinating agency for all other incidents involving foreign, unknown, or unlicensed radiological sources that have actual, potential, or perceived radiological consequences in the United States or its territories, possessions, or territorial waters. The foreign or unlicensed source may be a reactor, a spacecraft containing radioactive material, imported radioactively contaminated material, or a shipment of foreign-owned radioactive material. Unknown sources of radioactive material, also termed "orphan sources," are those materials whose origin and/or radiological nature are not yet established. These types of sources include contaminated scrap metal or abandoned radioactive material.

Other Types of Incidents: For other types of incidents not covered above, DHS, in consultation with the other coordinating agencies, designates a coordinating agency. If DHS determines that it is an Incident of National Significance, DHS is responsible for overall coordination and the designated coordinating agency assumes responsibilities as the coordinating agency.

Notification Procedures

- The owner/operator of a nuclear/radiological facility or owner/transporter of nuclear/ radiological material is generally the first to become aware of an incident and notifies State, local and tribal authorities and the coordinating agency.
- Federal, State, local, and tribal governments that become aware of a radiological incident from any source other than the coordinating agency notify the HSOC and the coordinating agency.
- The coordinating agency provides notification of a radiological incident to the HSOC and other coordinating agencies, as appropriate.
- Releases of hazardous materials that are regulated under the NCP (40 CFR part 302) are reported to the National Response Center.

Incident Actions

Headquarters: Incidents of National Significance

- Coordinating agencies and cooperating agencies report information and intelligence relative to situational awareness and incident management to the HSOC. Agencies with radiological response functions provide representatives to the HSOC, as requested.
- The coordinating agency and cooperating agencies, as appropriate, provide representation to the IIMG.
- Coordinating agencies and cooperating agencies provide representation to the National Response Coordination Center (NRCC), as appropriate.

Other Radiological Incidents

- For radiological incidents that are below the threshold of an Incident of National Significance but require Federal participation in the response, the coordinating agency coordinates the Federal response utilizing the procedures in this annex, agency-specific plans, and/or the NCP, as appropriate. The coordinating agency provides intelligence and information relative to the incident to the HSOC.
- The NRCC may be utilized to provide interagency coordination and Federal resource tracking, if needed.

Regional: Incidents of National Significance

- The coordinating agency provides representation to the JFO to serve as a Senior Federal Official within the JFO Coordination Group. Cooperating agencies may also be represented, as needed.
- The coordinating agency is part of the Unified Command, as defined by the NIMS, and coordinates Federal radiological response activities at appropriate field facilities.[2]

[2] Appropriate field facilities may include a JFO, Incident Command Post, Emergency Operations Center, Emergency Operations Facility, Emergency Control Center, etc.

Other Radiological Incidents: The coordinating agency coordinates Federal response operations at a designated field facility. Cooperating agencies may also be represented, as needed.

Response Functions: Primary radiological response functions are addressed in this section. An overview of specific DHS and coordinating agency response functions is provided in Table 2.

Table 2: DHS and coordinating agency response functions overview

Response Function	Incidents of National Significance	Other Radiological Incidents
a. Coordinate actions of Federal agencies related to the overall response.	DHS	Coordinating agency
b. Coordinate Federal activities related to response and recovery of the radiological aspects of an incident.	DHS and coordinating agency	Coordinating agency
c. Coordinate incident security.	DHS and coordinating agency	Coordinating agency
d. Ensure coordination of technical data (collection, analysis, storage, and dissemination).	DHS and coordinating agency	Coordinating agency
e. Ensure Federal protective action recommendations are developed and provide advice and assistance to State, local, and tribal governments.	DHS and coordinating agency	Coordinating agency
f. Coordinate release of Federal information to the public.	DHS	Coordinating agency
g. Coordinate release of Federal information to Congress.	DHS	Coordinating agency
h. Keep the White House informed on all aspects of an incident.	DHS	Coordinating agency
i. Ensure coordination of demobilization of Federal assets.	DHS	Coordinating agency

Response Coordination

Federal Agency Coordination

Incidents of National Significance	DHS is responsible for the overall coordination of Incidents of National Significance using elements described in the NRP Base Plan concept of operations.
Other Radiological Incidents	▪ The agency with primary responsibility for coordinating the Federal response to a radiological incident serves as the coordinating agency. ▪ The coordinating agency coordinates the actions of Federal agencies related to the incident utilizing this annex, agency-specific plans, and/or the NCP, as appropriate. ▪ Cooperating agencies provide technical and resource support, as requested by the coordinating agency. ▪ The coordinating agency may establish a field facility; assist State, local, and tribal response organizations; monitor and support owner/operator activities (when there is an owner or operator); provide technical support to the owner/operator, if requested; and serve as the principal Federal source of information about incident conditions.

Coordinating Radiological Aspects of an Incident

Incidents of National Significance	▪ DHS and the coordinating agency coordinate Federal activities related to responding to and recovering from the radiological aspects of an incident. They are assisted by cooperating agencies, as requested. ▪ The coordinating agency provides a hazard assessment of conditions that might have significant impact and ensures that measures are taken to mitigate the potential consequences.
Other Radiological Incidents	The coordinating agency coordinates Federal activities related to response and recovery of the radiological aspects of an incident, assisted by cooperating agencies, as requested.

Incident Security Coordination

Incidents of National Significance	DHS and the coordinating agency are responsible for coordinating security activities related to Federal response operations.
Other Radiological Incidents	The coordinating agency coordinates security activities related to Federal response operations.

Incident Security Coordination (Continued)

Incidents of National Significance and Other Radiological Incidents	▪ DOD, DOE, or NASA, as the appropriate coordinating agency, may establish NDAs or NSAs to safeguard classified information and/or restricted data, or equipment and material, and place non-Federal lands under Federal control for the duration of the incident. DOD, DOE, or NASA, as appropriate, coordinates security in and around these locations, as necessary. ▪ For incidents at other Federal or private facilities, the owner/operator provides security within the facility boundaries. If a release of radioactive material occurs beyond the facility boundaries, State, local, or tribal governments provide security for the release area. ▪ State, local, and tribal governments provide security for radiological incidents occurring on public lands (e.g., a transportation incident). ▪ If needed, ESF #13 – Public Safety and Security may be activated to provide supplemental security resources and capabilities.

Technical Data Management

Incidents of National Significance	▪ DHS and the coordinating agency approve the release of all data to State, local, and tribal governments. ▪ For incidents involving terrorism, the coordinating agency consults with other members of the JFO Coordination Group as issues arise regarding the sharing of sensitive information that may be needed, on a need-to-know basis, for responder and public safety. ▪ DHS and the coordinating agency, in consultation with the JFO Coordination Group and State, local, and tribal governments, determine if the severity of an incident warrants a request for Nuclear Incident Response Team (NIRT) assets. ▪ The IMAAC is responsible for production, coordination, and dissemination of consequence predictions for an airborne hazardous material release. The IMAAC generates the single Federal prediction of atmospheric dispersions and their consequences utilizing the best available resources from the Federal Government.
Other Radiological Incidents	The coordinating agency authorizes the release of all data to State, local, and tribal governments.

Technical Data Management (Continued)

Incidents of National Significance and Other Radiological Incidents	▪ The coordinating agency oversees the collection, analysis, storage, and dissemination of all technical data through the entire process. ▪ The coordinating agency is responsible for ensuring the sharing of all technical data, including outputs from the FRMAC, the Advisory Team, and the IMAAC, with all appropriate response organizations. ▪ Federal monitoring and assessment activities are coordinated with State, local, and tribal governments. Federal agency plans and procedures for implementing this activity are designed to be compatible with the radiological emergency planning requirements for State and local governments, specific facilities, and existing memorandums of understanding and interagency agreements. ▪ Prior to the on-scene arrival of the coordinating agency, Federal first responders may provide radiological monitoring and assessment data to State, local, and tribal governments as requested in support of protective action decisionmaking. Federal first responders also begin collecting data for transmission to the coordinating agency. If a FRMAC is established, the coordinating agency provides a mechanism for transmitting data to and from the FRMAC. Prior to the initiation of FRMAC operations, Federal first responders coordinate radiological monitoring and assessment data with the DOE Consequence Management Home Team (CMHT) or the Consequence Management Response Team (CMRT). (Note: A CMHT provides a reach-back capability to support the CMRT. The CMRT functions as an advance element of the FRMAC to establish contact with on-scene responders to coordinate Federal radiological monitoring and assessment activities.) ▪ DOE and other participating Federal agencies learn of an emergency when they are alerted to a possible problem or receive a request for radiological assistance. DOE maintains national and regional coordination offices as points of access to Federal radiological emergency assistance. Requests for Radiological Assessment Program (RAP) teams are generally directed to the appropriate DOE Regional Coordinating Office. All other requests for Federal radiological monitoring and assessment go directly to DOE's Emergency Operations Center (EOC) in Washington, DC. When other agencies receive requests for Federal radiological monitoring and assessment assistance, they notify the DOE EOC.

Technical Data Management (Continued)

Incidents of National Significance and Other Radiological Incidents (Continued)	▪ DOE may respond to a State or coordinating agency request for assistance by dispatching a RAP team. If the situation requires more assistance than a RAP team can provide, DOE alerts or activates additional resources. These resources can include the establishment of a FRMAC as the coordination center for Federal radiological assessment activities. DOE may respond with additional resources including the Aerial Measurement System (AMS) to provide wide-area radiation monitoring, Radiation Emergency Assistance Center/Training Site (REAC/TS) medical advisory teams, National Atmospheric Release Advisory Center (NARAC) support, or if the accident involves a U.S. nuclear weapon, the Accident Response Group (ARG). Federal and State agencies are encouraged to collocate their radiological assessment activities. Some participating Federal agencies have radiological planning and emergency responsibilities as part of their statutory authority, as well as established working relationships with State counterpart agencies. The monitoring and assessment activity, coordinated by DOE, does not alter these responsibilities but complements them by providing for coordination of the initial Federal radiological monitoring and assessment response activity. ▪ Responsibility for coordinating radiological monitoring and assessment activities may transition to EPA at a mutually agreeable time, and after consultation with State, local, and tribal governments, the coordinating agency, and the JFO Coordination Group.

Protective Action Recommendations

Incidents of National Significance	DHS and the coordinating agency oversee the development of Federal Protective Action Recommendations and provide advice and assistance to State, tribal, and local governments. Federal Protective Action Recommendations are developed by the Advisory Team, in conjunction with the coordinating agency. Federal Protective Action Recommendations may include advice and assistance on measures to avoid or reduce exposure of the public to radiation from a release of radioactive material. This includes advice on emergency actions such as sheltering, evacuation, and prophylactic use of potassium iodide. It also includes advice on long-term measures, such as restriction of food, temporary relocation, or permanent resettlement, to avoid or minimize exposure to residual radiation or exposure through the ingestion pathway.
Other Radiological Incidents	The coordinating agency, in consultation with the Advisory Team, develops and provides Protective Action Recommendations.
Incidents of National Significance and Other Radiological Incidents	State, local, and tribal governments are responsible for implementing protective actions as they deem appropriate.

Public Information Coordination

Incidents of National Significance and Other Radiological Incidents	DHS, in consultation with other agencies and the JFO Coordination Group oversees and manages the establishment of a Joint Information Center (JIC), if required.
Other Radiological Incidents	The coordinating agency may establish a JIC depending on the needs of the incident response.
Incidents of National Significance and Other Radiological Incidents	▪ Owners/operators and Federal, State, local, tribal, and other relevant information sources coordinate public information to the extent practical with the JIC. Communication with the public is accomplished in accordance with procedures outlined in the ESF #15 – External Affairs Annex and the Public Affairs Support Annex. ▪ It may be necessary to release Federal information regarding public health and safety. In this instance, Federal agencies coordinate with the coordinating agency and State, local, and tribal governments in advance, or as soon as possible after the information is released.

Congressional Coordination

Incidents of National Significance	DHS coordinates Federal responses to congressional requests for information. Points of contact for this function are the congressional liaison officers. All Federal agency congressional liaison officers and congressional staffs seeking site-specific information about an incident should contact the DHS Office of Legislative Affairs and the coordinating agency. While Congress may request information directly from any Federal agency, any agency responding to such requests shall inform DHS and the coordinating agency.
Other Radiological Incidents	The coordinating agency is responsible for congressional coordination, consulting with DHS as required.

White House Coordination

Incidents of National Significance	DHS submits reports to the President and keeps the White House informed of all aspects of the incident. While the White House may request information directly from any Federal agency, any agency responding to such requests must promptly inform DHS and the coordinating agency.
Other Radiological Incidents	The coordinating agency is responsible for any necessary White House coordination, consulting with DHS as requested. Note that these actions can take place during the transition from response to recovery.

Deactivation/Demobilization Coordination

Incidents of National Significance	DHS and the coordinating agency, in consultation with the JFO Coordination Group and State, local, and tribal governments, develop plans to demobilize the Federal presence.
Other Radiological Incidents	The coordinating agency discontinues incident operations when a centralized Federal coordination presence is no longer required, or when its statutory responsibilities are fulfilled. Prior to discontinuing operations, the coordinating agency coordinates this decision with each Federal agency and State, local, and tribal governments.

International Coordination

Incidents of National Significance and Other Radiological Incidents	▪ In the event of an actual or potential environmental impact upon the United States or its possessions, territories, or territorial waters from a radiological emergency originating on foreign soil or, conversely, a domestic incident with an actual or potential foreign impact, DHS and the coordinating agency immediately inform the Department of State (DOS), which is responsible for official interactions with foreign governments. In either case (foreign incident with domestic impact, or vice versa), the coordinating agency consults with DHS, and DHS makes a determination on whether it is an Incident of National Significance. DHS and the coordinating agency keep DOS informed of all Federal incident management activities. ▪ DOS coordinates notification and information-gathering activities with foreign governments, except in cases where existing bilateral agreements permit direct communication. Where the coordinating agency has existing bilateral agreements that permit direct exchange of information, the coordinating ageney keeps DOS informed of consultations with their foreign counterparts. DHS and the coordinating agency ensure that any offers of assistance to, or requests from, foreign governments are coordinated with DOS. ▪ The National Oceanic and Atmospheric Administration is the point of interaction with the hydrometeorological services of other countries. International response activities are accomplished in accordance with the International Coordination Support Annex.

Victim Decontamination/Population Monitoring

Incidents of National Significance and Other Radiological Incidents	▪ External monitoring and decontamination of possibly affected victims are accomplished locally and are the responsibility of State, local, and tribal governments. Federal resources are provided at the request of, and in support of, the affected State(s). HHS, through ESF #8 and in consultation with the coordinating agency, coordinates Federal support for external monitoring of people and decontamination. ▪ HHS assists and supports State, local, and tribal governments in performing monitoring for internal contamination and administering available pharmaceuticals for internal decontamination, as deemed necessary by State health officials. ▪ HHS assists local and State health departments in establishing a registry of potentially exposed individuals, perform dose reconstruction, and conduct long-term monitoring of this population for potential long-term health effects.

Other Federal Resource Support

For Stafford Act or Federal-to-Federal support incidents, DHS/EPR/FEMA coordinates the provision of Federal resources and assistance to affected State, local, and tribal governments as part of the JFO Operations Section or other appropriate location established by DHS/EPR/FEMA.

Recovery

- For an Incident of National Significance, DHS coordinates overall Federal recovery activities, while the coordinating agency maintains responsibility for managing the Federal technical radiological cleanup activities in accordance with NRP mechanisms.

- For all radiological incidents, the coordinating agency coordinates environmental remediation/cleanup in concert with cognizant State, local, and tribal governments, and owners/operators, as applicable. While retaining overall technical lead, a coordinating agency may require support from a cooperating agency that has significant cleanup/recovery experience and capabilities (e.g., EPA, U.S. Army Corps of Engineers (USACE)) for a long-term cleanup. The initial coordinating agency may request that the coordinating agency role be transitioned to a cooperating agency to manage long-term cleanup efforts.

- State, local, and tribal governments primarily are responsible for planning the recovery of the affected area (the term "recovery," as used here, encompasses any action dedicated to the continued protection of the public and resumption of normal activities in the affected area). Recovery planning is initiated at the request of the State, local, or tribal governments, and generally does not take place until the initiating conditions of the incident have stabilized and immediate actions to protect public health, safety, and property are accomplished. Upon request, the Federal government assists State, local, and tribal governments develop and execute recovery plans.

- Private owners/operators have primary responsibility for recovery planning activities and eventual cleanup within their facility boundaries and may have responsibilities for recovery activities outside their facility under applicable legal obligations (e.g., contractual, licensee, CERCLA).

- The DOE FRMAC Director works closely with the Senior EPA representative to facilitate a smooth transition of the Federal radiological monitoring and assessment coordination responsibility to EPA at a mutually agreeable time, and after consultation with DHS, the JFO Coordination Group, and State, local, and tribal

governments. The following conditions are intended to be met prior to transfer:

- The immediate emergency condition is stabilized;
- Offsite releases of radioactive material have ceased, and there is little or no potential for further unintentional offsite releases;
- The offsite radiological conditions are characterized and the immediate consequences are assessed;
- An initial long-range monitoring plan has been developed in conjunction with the affected State, local, and tribal governments and appropriate Federal agencies; and
- EPA has received adequate assurances from the other Federal agencies that they are committing the required resources, personnel, and funds for the duration of the Federal response.

- Radiological monitoring and assessment activities are normally terminated when DHS, in consultation with the coordinating agency, other participating agencies, and State, local, and tribal governments, determines that:
  - There is no longer a threat to public health and safety or the environment;
  - State, local, and tribal resources are adequate for the situation; and
  - There is mutual agreement among the agencies involved to terminate monitoring and assessment.

Federal Assets Available Upon Request by the Coordinating Agency or DHS

Federal Radiological Monitoring and Assessment Center

DOE is responsible for developing and maintaining FRMAC policies and procedures, determining FRMAC composition, and maintaining FRMAC operational readiness. The FRMAC is established at or near the incident location in coordination with DHS, the coordinating agency, other Federal agencies, and State, local, and tribal authorities. A FRMAC normally includes representation from DOE, EPA, the Department of Commerce, the National Communications System (DHS/IAIP/NCS), USACE, and other Federal agencies as needed. Regardless of who is designated as the coordinating agency, DOE, through the FRMAC or DOE CMHT and CMRT, coordinates radiological monitoring and assessment activities for the initial phases of the response. When the FRMAC is transferred to the EPA, they assume responsibility for coordination of radiological monitoring and assessment activities.

Advisory Team for Environment, Food, and Health

- The Advisory Team includes representatives from DHS, EPA, the Department of Agriculture (USDA), the Food and Drug Administration, the Centers for Disease Control and Prevention, and other Federal agencies. The Advisory Team develops coordinated advice and recommendations for DHS, the JFO Coordination Group, the coordinating agency, and State, local, and tribal governments concerning environmental, food health, and animal health matters.
- The Advisory Team selects a chair for the Team.
- The Advisory Team provides recommendations in matters related to the following:
  - Environmental assessments (field monitoring) required for developing recommendations with advice from State, local, and tribal governments and/or the FRMAC senior Monitoring Manager;
  - Protective Action Guides and their application to the emergency;
  - Protective Action Recommendations using data and assessment from the FRMAC;
  - Protective actions to prevent or minimize contamination of milk, food, and water, and to prevent or minimize exposure through ingestion;

- Recommendations regarding the disposition of contaminated livestock, poultry, and contaminated foods, especially perishable commodities (e.g., meat in processing plants);
- Recommendations for minimizing losses of agricultural resources from radiation effects;
- Availability of food, animal feed, and water supply inspection programs to assure wholesomeness;
- Relocation, reentry, and other radiation protection measures prior to recovery;
- Recommendations for recovery, return, and cleanup issues;
- Health and safety advice or information for the public and for workers;
- Estimated effects of radioactive releases on human health and the environment; and
- Other matters, as requested by the coordinating agency.

DOE Radiological Assistance Program, Emergency Management Teams, and Nuclear Incident Response Team Assets

- RAP teams are located at DOE operations offices, national laboratories, and some area offices. They can be dispatched to a radiological incident by the DOE regional coordinating offices responding to a radiological incident.

Additional DOE planning and response teams and capabilities are located at various DOE facilities throughout the country and can be dispatched, as needed, to a radiological incident.

Responsibilities

American Red Cross	(See the ESF #6 – Mass Care, Housing, and Human Services Annex for additional information.) Assesses the mass care consequences of a radiological incident, and in conjunction with State, local, and tribal (including private-sector) mass care organizations, develop and implement a sustainable short-term and long-term strategy for effectively addressing the consequences of the incident.
Department of Agriculture	(See the ESF #11 – Agriculture and Natural Resources Annex for additional information.) ▪ Inspects meat and meat products, poultry and poultry products, and egg products identified for interstate and foreign commerce to ensure that they are safe for human consumption. ▪ Assists, in conjunction with HHS, in monitoring the production, processing, storage, and distribution of food through the wholesale level to eliminate contaminated product or to reduce the contamination in the product to a safe level. ▪ Collects agricultural samples within the Ingestion Exposure Pathway Emergency Planning Zone (through the FRMAC). Assists in the evaluation and assessment of data to determine the impact of the incident on agriculture. ▪ Assesses damage to crops, soil, livestock, poultry, and processing facilities and incorporates findings in a damage assessment report. ▪ Provides emergency communications assistance to the agricultural community through the State Research, Education, and Extension Services electronic mail, or other USDA telecommunications systems. ▪ Supports/advises on decontamination and screening of pets and farm animals that may be exposed to radioactive material. ▪ Assists in animal carcass disposal.
Department of Commerce	▪ Provides operational weather observations and prepares forecasts tailored to support emergency incident management activities. ▪ Provides plume dispersion assessment and forecasts to the IMAAC and/or coordinating agency, in accordance with established procedures. ▪ Archives, as a special collection, the meteorological data from national observing and numerical weather analysis and prediction systems applicable to the monitoring and assessment of the response. ▪ Ensures that marine fishery products available to the public are not contaminated. ▪ Provides assistance and reference material for calibrating radiological instruments. ▪ Provides radiation shielding materials. ▪ In the event of materials potentially crossing international boundaries, serves as the agent for informing international hydrometeorological services and associated agencies through the mechanisms afforded by the World Meteorological Organization. ▪ Provides radioanalytical measurement support and instrumentation.

Department of Defense	▪ Serves as a coordinating agency, as identified in Table 1, coordinating Federal actions for radiological incidents involving DOD facilities, including U.S. nuclear-powered ships, or material otherwise under their jurisdiction (e.g., transportation of material shipped by or for DOD). ▪ Provides Defense Support of Civil Authorities (DSCA) in response to requests for assistance during domestic incidents. With the exception for support provided under Immediate Response Authority, the obligation of DOD resources to support requests for assistance is subject to the approval of the Secretary of Defense. Details regarding DSCA are provided in the NRP Base Plan. ▪ Provides Immediate Response Authority under imminently serious conditions resulting from any civil emergency that may require immediate action to save lives, prevent human suffering, or mitigate great property damage. When such conditions exist and time does not permit prior approval from higher headquarters, local military commanders and responsible officials from DOD components and agencies are authorized by DOD directive, subject to any supplemental direction that may be provided by their DOD component, to take necessary action to respond to requests of civil authorities. All such necessary action is referred to as "Immediate Response."

Department of Defense/U.S. Army Corps of Engineers	(See the ESF #3 – Public Works and Engineering Annex for additional information.)
	▪ Directs response/recovery actions as they relate to ESF #3 functions, including contaminated debris management.
	▪ For RDD/IND incidents, provides response and cleanup support as a cooperating agency.
	▪ Integrates and coordinates with other agencies, as requested, to perform any or all of the following:
	  ▪ Radiological survey functions;
	  ▪ Gross decontamination;
	  ▪ Site characterization;
	  ▪ Contaminated water management; and
	  ▪ Site remediation.

Department of Energy	▪ Serves as a coordinating agency, as identified in Table 1, coordinating Federal actions for radiological incidents involving DOE facilities or material otherwise under their jurisdiction (e.g., transportation of material shipped by or for DOE). ▪ Coordinates Federal offsite radiological environmental monitoring and assessment activities as lead technical organization in FRMAC (emergency phase), regardless of who is designated the coordinating agency. ▪ Maintains technical liaison with State and local agencies with monitoring and assessment responsibilities. ▪ Maintains a common set of all offsite radiological monitoring data in an accountable, secure, and retrievable form and ensures the technical integrity of FRMAC data. ▪ Provides monitoring data and interpretations, including exposure rate contours, dose projections, and any other requested radiological assessments, to the coordinating agency and to the States. ▪ Provides, in cooperation with other Federal agencies, the personnel and equipment to perform radiological monitoring and assessment activities, and provides on-scene analytical capability supporting assessments. ▪ Requests supplemental assistance and technical support from other Federal agencies as needed. ▪ Arranges consultation and support services through appropriate Federal agencies to all other entities (e.g., private contractors) with radiological monitoring functions and capabilities and technical and medical expertise for handling radiological contamination and population monitoring. ▪ Works closely with the Senior EPA representative to facilitate a smooth transition of the Federal radiological monitoring and assessment coordination responsibility to EPA at a mutually agreeable time and after consultation with the States and coordinating agency. ▪ Provides, in cooperation with other Federal and State agencies, personnel and equipment, including portal monitors, to support initial external screening and provides advice and assistance to State and local personnel conducting screening/decontamination of persons leaving a contaminated zone. ▪ Provides plume trajectories and deposition projections for emergency response planning assessments including source term estimates where limited or no information is available, including INDs and RDDs, to the IMAAC and/or coordinating agency, in accordance with established procedures. ▪ Upgrades, maintains, coordinates, and publishes documentation needed for the administration, implementation, operation, and standardization of the FRMAC. ▪ Maintains and improves the ability to provide wide-area radiation monitoring now resident in the AMS. ▪ Maintains and improves the ability to provide medical assistance, advisory teams, and training related to nuclear/radiological accidents and incidents now resident in the REAC/TS.

Department of Energy (Continued)	▪ Maintains and improves the ability to provide near-real time assessments of the consequences of accidental or potential radiation releases by modeling the movement of hazardous plumes, and to correct modeled results through integration of actual radiation measurements obtained from both airborne and ground sources, resident in the NARAC. The NARAC also maintains and improves their ability to model the direct results (blast, thermal, radiation, EMP) of a nuclear detonation. ▪ Maintains and improves the first-response ability to assess an emergency situation and to advise decisionmakers on what further steps can be taken to evaluate and minimize the hazards of a radiological emergency resident in the RAP. ▪ Maintains and improves the ability to respond to an emergency involving U.S. nuclear weapons resident in the ARG. ▪ Maintains and improves the ability of the Consequence Management Planning Team, CMHT, and CMRTs to provide initial planning, coordination, and data collection and assessment prior to or in lieu of establishment of a FRMAC. ▪ Maintains and improves the ability of the Nuclear/Radiological Advisory Team to provide advice and limited technical assistance, including search, diagnostics, and effects prediction, as part of a Domestic Emergency Support Team. ▪ Maintains and improves the ability of the Search Response Teams to provide covert search capability using local support for initial nuclear search activities. ▪ Maintains and improves the ability of the Joint Technical Operations Team to provide technical operations advisory support and advanced technical assistance to the Federal primary or coordinating agency, provide extended technical support to other deployed operations through an emergency response home team; perform nuclear safety reviews to determine safe-to-ship status before moving a weapon of mass destruction (WMD) to an appropriate disposal location; and accept custody of nuclear or radiological WMD on behalf of DOE and provide for the final disposition of these devices. ▪ Maintains and improves the ability of Radiological Triage to determine through remote analysis of nuclear spectra collected on-scene if a radioactive object contains special nuclear materials. ▪ Assigns a Senior Energy Official (SEO) for any response involving the deployment of the DOE/NNSA emergency response assets. The SEO is responsible for the coordination and employment of these assets at the scene of a radiological event, and the deployed assets will work in support of and under the direction of the SEO.

Department of Health and Human Services	(See the ESF #8 – Public Health and Medical Services Annex for additional information.) ▪ In conjunction with USDA, inspects production, processing, storage, and distribution facilities for human food and animal feeds that may be used in interstate commerce to ensure protection of the public health. ▪ Collects samples of agricultural products to monitor and assess the extent of contamination as a basis for recommending or implementing protective actions (through the FRMAC). ▪ Provides advice on proper medical treatment of the general population and response workers exposed to or contaminated by radioactive materials. ▪ Provides available medical countermeasures through deployment of the Strategic National Stockpile. ▪ Provides assessment and treatment teams for those exposed to or contaminated by radiation. ▪ Provides advice and guidance in assessing the impact of the effects of radiological incidents on the health of persons in the affected area. ▪ Manages long-term public monitoring and supports follow-on personal data collection, collecting and processing of blood samples and bodily fluids/matter samples, and advice concerning medical assessment and triage of victims. Tracks victim treatment and long-term health effects.
Department of Homeland Security/Emergency Preparedness and Response/Federal Emergency Management Agency	▪ Serves as the annex coordinator for this annex. ▪ In consultation with the coordinating agency, coordinates the provision of Federal resources and assistance to affected State, local, and tribal governments under the Stafford Act or Federal-to-Federal support provisions of the NRP. ▪ Monitors the status of the Federal response to requests for assistance from the affected State(s) and provides this information to the State(s). ▪ Keeps the coordinating agency informed of requests for assistance from the State(s) and the status of the Federal response. ▪ Identifies and informs Federal agencies of actual or apparent omissions, redundancies, or conflicts in response activity. ▪ Establishes and maintains a source of integrated, coordinated information about the status of all nonradiological resource support activities. ▪ Provides other support to Federal agencies responding to the emergency.
Department of Homeland Security/National Communications System	(See the ESF #2 – Communications Annex for additional information.) Acting through its operational element, the National Coordinating Center for Telecommunications (NCC), the NCS ensures the provision of adequate telecommunications support to Federal radiological incident response operations.
Department of Homeland Security/Science and Technology	(See the Science and Technology Support Annex for additional information.) Provides coordination of Federal science and technology resources as described in the Science and Technology Support Annex. This includes organization of Federal S&T support as well as assessment and consultation in the form of Scientific and Technical Advisory and Response Teams (START s) and the IMAAC.

Department of Homeland Security/Customs and Border Protection (DHS/CBP)	▪ For incidents at the border, maintains radiation detection equipment and nonintrusive inspection technology at ports of entry and Border Patrol checkpoints to detect the presence of radiological substances transported by persons, cargo, mail, or conveyance arriving from foreign countries. ▪ Through its National Targeting Center, provides extensive analytical and targeting capabilities to identify and interdict terrorists and WMD. ▪ The CBP Weapons of Mass Destruction Teleforensic Center provides 24/7 support to DHS/CBP and other Federal law enforcement personnel in the identification of suspect hazardous material. ▪ The CBP Laboratory and Scientific Services staffs WMD Response Teams in strategic locations nationwide. ▪ Through the Container Security Initiative, DHS/CBP personnel are stationed at major foreign seaports in order to detect and prevent the transport of WMD on container vessels destined to the U.S. ▪ Has extensive authority and expertise regarding the entry, inspection, and admissibility of persons, cargo, mail, and conveyances arriving from foreign countries.

Department of Homeland Security/U.S. Coast Guard	▪ Serves as coordinating agency for incidents that occur in certain areas of the coastal zone, as identified in Table 1.
	▪ "Certain areas of the coastal zone," for the purposes of this document, means the following areas of the coastal zone as defined by the NCP:
	  ▪ Vessels, as defined in 33 CFR 160;
	  ▪ Areas seaward of the shoreline to the outer edge of the Economic Exclusion Zone; and
	  ▪ Within the boundaries of the following waterfront facilities subject to the jurisdiction of DHS/USCG; those regulated by 33 CFR 126 (Dangerous cargo handling), 127 (LPG/LNG), 128 (Passenger terminals), 140 (Outer Continental Shelf Activities), 1541-56 (Waterfront portions of Oil & Hazmat bulk transfer facilities – delineated as per the NCP), 105 (Maritime security - facilities).
	EPA is the coordinating agency for responses in areas of the coastal zone other than those defined above as certain areas of the coastal zone.
	▪ For incidents that have cross-boundary impacts, works with the other affected agency to determine how best to cooperatively respond consistent with the NCP model.
	▪ Serves as the coordinating agency for these incidents only during the prevention and emergency response phase, and transfers responsibility for later response phases to the appropriate agency, consistent with the NCP.
	▪ Because of its unique maritime jurisdiction and capabilities, is prepared to provide appropriate security, command and control, transportation, and support to other agencies that need to operate in the maritime domain.

Department of Housing and Urban Development	▪ Reviews and reports on available housing for disaster victims and displaced persons. ▪ Assists in planning for and placing homeless victims in available housing ▪ Provides staff to support emergency housing within available resources. ▪ Provides housing assistance and advisory personnel.
Department of the Interior (DOI)	▪ Advises and assists in evaluating processes affecting radioisotopes in soils, including personnel, equipment, and laboratory support. ▪ Advises and assists in the development of geographic information systems databases to be used in the analysis and assessment of contaminated areas, including personnel and equipment. ▪ Advises and assists in assessing and dealing with impacts to natural resources, including fish and wildlife, subsistence uses, public lands, Indian tribal lands, land reclamation, mining, minerals, and water resources. Further guidance is provided in the Tribal Relations Support Annex and the ESF #11 – Agriculture and Natural Resources Annex. ▪ Provides liaison between federally recognized tribal governments and Federal, State, and local agencies for coordination of response activities. Additionally, DOI advises and assists DHS on economic, social, and political matters in the U.S. insular areas should a radiological incident occur in these areas.
Department of Justice/Federal Bureau of Investigation	Coordinates all law enforcement and criminal investigative response to acts of terrorism, to include intelligence gathering, hostage negotiations, and tactical operations. Further details regarding the FBI response are outlined in the Terrorism Incident Law Enforcement and Investigation Annex.
Department of Labor/Occupational Safety and Health Administration	Provides advice and technical assistance to DHS, the coordinating agency, and State, local, and tribal governments concerning the health and safety of response workers implementing the policies and concepts in this annex.
Department of State	▪ Coordinates foreign information-gathering activities and all contacts with foreign governments, except in cases where existing bilateral agreements permit direct agency-to-agency cooperation. ▪ Conveys the U.S. Government response to foreign offers of assistance.
Department of Transportation	(See the ESF #1 – Transportation Annex for further information.) Provides technical advice and assistance on the transportation of radiological materials and the impact of the incident on the transportation infrastructure.
Department of Veterans Affairs	▪ Provides medical assistance using the Medical Emergency Radiological Response Team. ▪ Provides temporary housing.

Environmental Protection Agency	(See the Hazardous Materials Incident Annex for additional information.) ▪ Serves as a coordinating agency, as identified in Table 1. ▪ Provides resources, including personnel, equipment, and laboratory support (including mobile laboratories) to assist DOE in monitoring radioactivity levels in the environment. ▪ Assumes coordination of Federal radiological monitoring and assessment responsibilities after the transition from DOE. ▪ Assists in the development and implementation of a long-term monitoring plan and long-term recovery plan. ▪ Provides nationwide environmental monitoring data from the Environmental Radiation Ambient Monitoring Systems for assessing the national impact of the incident. ▪ Develops Protective Action Guides in coordination with the FRPCC. ▪ Recommends protective actions and other radiation protection measures. ▪ Recommends acceptable emergency levels of radioactivity and radiation in the environment. ▪ Prepares health and safety advice and information for the public. ▪ Estimates effects of radioactive releases on human health and the environment. ▪ Provides response and recovery actions to prevent, minimize, or mitigate a threat to public health, safety, or the environment caused by actual or potential releases of radioactive substances, including actions to detect, identify, contain, clean up, and dispose of such substances. ▪ Assists and supports the NIRT, when activated. ▪ Provides, in cooperation with other Federal agencies, the law enforcement personnel and equipment to conduct law enforcement operations and investigations for nuclear/radiological incidents involving criminal activity that are not terrorism related.
General Services Administration	(See the ESF #7 – Resource Support Annex for additional information.)
National Aeronautics and Space Administration	Serves as a coordinating agency, as identified in Table 1.

Nuclear Regulatory Commission	▪ Serves as a coordinating agency, as identified in Table 1.
	▪ Provides technical assistance to include source term estimation, plume dispersion, and dose assessment calculations.
	▪ Provides assistance and recommendations concerning protective action measures as coordinating agency.
	▪ Provides assistance in Federal radiological monitoring and assessment activities.
	▪ For an incident at a facility licensed by the NRC or an Agreement State, or involving Atomic Energy Act licensed material:
	▪ The licensee takes action to mitigate the consequences of the incident and provides appropriate protective action recommendations to State, local, and tribal officials;
	▪ The NRC:
	  ▪ Performs an independent assessment of the incident and potential offsite consequences and, as appropriate, provides recommendations concerning any protective measures;
	  ▪ Performs oversight of the licensee, to include monitoring, evaluation of protective action recommendations, advice, assistance, and, as appropriate, direction; and
	  ▪ Dispatches, if appropriate, an NRC site team of technical experts to the licensee's facility.
	  ▪ Under certain situations involving the protection of public health/safety or national security, the NRC may take possession of special nuclear materials and/or operate certain facilities regulated by the NRC.

ENCLOSURE C

3. Biological Incident Annex

Biological Incident Annex

Coordinating Agency:

Department of Health and Human Services

Cooperating Agencies:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of Veterans Affairs
U.S. Agency for International Development
Environmental Protection Agency
General Services Administration
U.S. Postal Service
American Red Cross

Introduction

Purpose

The purpose of the Biological Incident Annex is to outline the actions, roles, and responsibilities associated with response to a disease outbreak of known or unknown origin requiring Federal assistance. Actions described in this annex take place with or without a Presidential Stafford Act declaration or a public health emergency declaration by the Secretary of Health and Human Services (HHS). This annex applies only to Incidents of National Significance. This annex outlines biological incident response actions including threat assessment notification procedures, laboratory testing, joint investigative/response procedures, and activities related to recovery.

Scope

The broad objectives of the Federal Government's response to a biological terrorism event, pandemic influenza, emerging infectious disease, or novel pathogen outbreak are to:

- Detect the event through disease surveillance and environmental monitoring;
- Identify and protect the population(s) at risk;
- Determine the source of the outbreak;
- Quickly frame the public health and law enforcement implications;
- Control and contain any possible epidemic (including providing guidance to State and local public health authorities);
- Augment and surge public health and medical services;
- Track and defeat any potential resurgence or additional outbreaks; and
- Assess the extent of residual biological contamination and decontaminate as necessary.

The unique attributes of this response require separate planning considerations that are tailored to specific health concerns and effects of the disease (e.g., terrorism versus natural outbreaks; communicable versus noncommunicable, etc.).

Specific operational guidelines, developed by the respective organizations to address the unique aspects of a particular disease or planning consideration, will supplement this annex and are intended as guidance to assist Federal, State, local, and tribal public health and medical planners.

Special Considerations

Detection of a bioterrorism act against the civilian population may occur in several different ways and involve several different modalities:

- An attack may be surreptitious, in which case the first evidence of dissemination of an agent may be the presentation of disease in humans or animals. This could manifest either in clinical case reports to domestic or international public health authorities or in unusual patterns of symptoms or encounters within domestic or international health surveillance systems.

- A terrorist-induced infectious disease outbreak initially may be indistinguishable from a naturally occurring outbreak; moreover, depending upon the particular agent and associated symptoms, several days could pass before public health and medical authorities even suspect that terrorism may be the cause. In such a case, criminal intent may not be apparent until some time after illnesses are recognized.

- Environmental surveillance systems, such as the BioWatch system, may detect the presence of a biological agent in the environment and trigger directed environmental sampling and intensified clinical surveillance to rule out or confirm an incident. If a case is confirmed, then these systems may allow for mobilization of a public health, medical, and law enforcement response in advance of the appearance of the first clinical cases or quick response after the first clinical cases are identified.

- The U.S. Postal Service may detect certain biological agents within the U.S. postal system. Detection of a biological agent in the mail stream triggers specific response protocols outlined in agency-specific standard operating procedures.

Policies

- This annex supports policies and procedures outlined in the ESF #8 – Public Health and Medical Services Annex, the ESF #10 – Oil and Hazardous Materials Response Annex, and the Terrorism Incident Law Enforcement and Investigation Annex.

- HHS serves as the Federal Government's primary agency for the public health and medical preparation and planning for and response to a biological terrorism attack or naturally occurring outbreak that results from either a known or novel pathogen, including an emerging infectious disease.

- State, local, and tribal governments are primarily responsible for detecting and responding to disease outbreaks and implementing measures to minimize the health, social, and economic consequences of such an outbreak.

- If any agency becomes aware of an overt threat involving biological agents or indications that instances of disease may not be the result of natural causes, the Department of Justice must be notified through the Federal Bureau of Investigation (FBI)'s Weapons of Mass Destruction Operations Unit (WMDOU). The FBI, in turn, immediately notifies the Department of Homeland Security (DHS) Homeland Security Operations Center (HSOC) and the National Counterterrorism Center (NCTC). The Laboratory Response Network (LRN) is used to test samples for the presence of biological threat agents. Decisions on where to perform additional tests on samples are made by the FBI, in coordination with HHS. (See the Terrorism Incident Law Enforcement and Investigation Annex for additional information on the FBI's roles and responsibilities.)

- Once notified of a credible threat or natural disease outbreak, HHS convenes a meeting of ESF #8 partners to assess the situation and determine appropriate public health and medical actions. DHS coordinates overall nonmedical support and response actions across all Federal departments and agencies. HHS coordinates overall public health and medical emergency response efforts across all Federal departments and agencies.

- Consistent with ESF #8, DHS closely coordinates the National Disaster Medical System (NDMS) medical response with HHS. The FBI coordinates the investigation of criminal activities if such activities are suspected.

- HHS provides guidance to State and local authorities and collaborates closely with the FBI in the proper handling of any materials that may have evidentiary implications (e.g., LRN samples, etc.) associated with disease outbreaks suspected of being terrorist or criminal in nature.

- Other Federal departments and agencies may be called upon to support HHS during the various stages of a disease outbreak response in the preparation, planning, and/or response processes.

- If there is potential for environmental contamination, HHS collaborates with the Environmental Protection Agency (EPA) in developing sampling strategies and sharing results.

- Given the dynamic nature of a disease outbreak, HHS, in collaboration with other departments and agencies, determines the thresholds for a comprehensive Federal Government public health and medical response. These thresholds are based on specific event information rather than predetermined risk levels.

- Any Federal public announcement, statement, or press release related to a threat or actual bioterrorism event must be coordinated with the DHS Public Affairs Office.

Planning Assumptions

- In a large disease outbreak, Federal, State, local, and tribal officials require a highly coordinated response to public health and medical emergencies. The outbreak also may affect other countries and therefore involve extensive coordination with the Department of State (DOS).

- Disease transmission can occur via an environmental contact such as atmospheric dispersion, person-to-person contact, animal-to-person contact, insect vector-to-person contact, or by way of contaminated food or water.

- A biological incident may be distributed across multiple jurisdictions simultaneously, requiring a nontraditional incident management approach. This approach could require the simultaneous management of multiple "incident sites" from national and regional headquarters locations in coordination with multiple State and local jurisdictions.

- A response to noncontagious public health emergencies may require different planning assumptions or factors.

- The introduction of biological agents, both natural and deliberate, are often first detected through clinical or hospital presentation. However, there are other methods of detection, including environmental surveillance technologies such as BioWatch and syndromic surveillance.

- No single entity possesses the authority, expertise, and resources to act unilaterally on the many complex issues that may arise in response to a disease outbreak and loss of containment affecting a multijurisdictional area. The national response requires close coordination with numerous agencies at all levels of government and the private sector.

- The Federal Government supports affected State, local, and tribal health jurisdictions as requested or required. The response by HHS and other Federal agencies is flexible and adapts as necessary as the outbreak evolves.

- The LRN provides for rapid public health assessment of the potential for human illness associated with exposure and the scope of this kind of risk. The LRN also addresses the need for law enforcement notification necessary to initiate threat assessment for criminal intent, and chain of custody procedures. Early HHS, FBI, and DHS coordination enhances the likelihood of successful preventative and investigative activities necessary to neutralize threats and attribute the source of the outbreak.

- Response to disease outbreaks suspected of being deliberate in origin requires consideration of special law enforcement and homeland security requirements.

- Test results from non-LRN facilities are considered a "first pass" or "screening" test (with the exception of the Legislative Branch, which has a separate lab system that is equivalent to LRN facilities).

- Any agency or organization that identifies an unusual or suspicious test result should contact the FBI to ensure coordination of appropriate testing at an HHS-certified LRN laboratory.

- HHS has identified specific Department of Defense laboratories that meet the standards and requirements for LRN membership.

- All threat and public health assessments are provided to the HSOC.

Concept of Operations

Biological Agent Response

The key elements of an effective biological response include (in nonsequential order):

- Rapid detection of the outbreak;

- Swift agent identification and confirmation;

- Identification of the population at risk;

- Determination of how the agent is transmitted, including an assessment of the efficiency of transmission;

- Determination of susceptibility of the pathogen to treatment;

- Definition of the public health, medical, and mental health implications;

- Control and containment of the epidemic;

- Decontamination of individuals, if necessary;

- Identification of the law enforcement implications/assessment of the threat;

- Augmentation and surging of local health and medical resources;

- Protection of the population through appropriate public health and medical actions;

- Dissemination of information to enlist public support;

- Assessment of environmental contamination and cleanup/decontamination of bioagents that persist in the environment; and

- Tracking and preventing secondary or additional disease outbreak.

Primary Federal functions include supporting State, local, and tribal public health and medical capacities according to the policies and procedures detailed in the NRP Base Plan and the ESF #8 Annex.

Suspicious Substances

Since there is no definitive/reliable field test for biological agents, all potential bioterrorism samples are transported to an LRN laboratory, where expert analysis is conducted using established HHS/Centers for Disease Control and Prevention (CDC) protocols/reagents. A major component of this process is to establish and maintain the law enforcement chain of custody and arrange for transport.

The following actions occur if a positive result is obtained by an LRN on an environmental sample submitted by the FBI or other designated law enforcement personnel:

- The LRN immediately notifies the local FBI of the positive test result;

- The FBI Field Office makes local notifications and contacts the FBI Headquarters WMDOU;

- FBI Headquarters convenes an initial conference call with the local FBI and HHS to review the results, assess the preliminary information and test results, and arrange for additional testing;

- FBI Headquarters immediately notifies DHS of the situation;

- Original samples may be sent to HHS/CDC for confirmation of LRN analyses;

- HHS provides guidance on protective measures such as prophylactic treatment and continued facility operation; and

- HHS and cooperating agencies support the determination of the contaminated area, decisions on whether to shelter in place or evacuate, and decontamination of people, facilities, and outdoor areas.

Outbreak Detection

Determination of a Disease Outbreak

The initial indication of a major disease outbreak, intentional or naturally occurring, may be the recognition by public health and medical authorities that a significantly increased number of people are becoming ill and presenting to local healthcare providers. Therefore, the most critical decisionmaking support requires surveillance information, identification of the causative biological agent, a determination of whether the observations are or are not related to a naturally occurring outbreak, and the identification of the population(s) at risk.

Laboratory Confirmation

During the evaluation of a suspected disease outbreak, laboratory samples are distributed to appropriate laboratories. During a suspected terrorist event, sample information is provided to the FBI for investigative use and to public health and emergency response authorities for epidemiological use and agent characterization to facilitate and ensure timely public health and medical interventions. If the incident begins as an epidemic of unknown origin detected through Federal, State, local, or tribal health surveillance systems or networks, laboratory analysis is initiated through the routine public health laboratory network.

Identification (Analysis and Confirmation)

The samples being collected and the analyses being conducted must be sufficient to characterize the cause of the outbreak. LRN laboratories fulfill the Federal responsibility for rapid analysis of biological agents. In a suspected terrorism event, sample collection activities and testing are coordinated with FBI and LRN member(s).

Notification

Any disease outbreak suspected or identified by an agency within HHS or through another Federal public health partner is brought to the immediate attention of the HHS Assistant Secretary for Public Health Emergency Preparedness as detailed in the ESF #8 Annex or internal HHS policy documents, in addition to the notification requirements contained in the NRP Base Plan.

Following these initial notifications, the procedures detailed in the ESF #8 Annex are followed. Instances of disease that raise the "index of suspicion," as determined by HHS, are reported to FBI Headquarters. In these instances, FBI Headquarters, in conjunction with HHS, examines available law enforcement and intelligence information, as well as the technical characteristics and epidemiology of the disease, to determine if there is a possibility of criminal intent. If the FBI, in conjunction with HHS, determines that the information represents a potential credible terrorist threat, the FBI communicates the situation to the HSOC, which notifies the White House, as appropriate. If warranted, the FBI, HHS, and State, local, and tribal health officials conduct a joint law enforcement and epidemiological investigation to determine the cause of the disease outbreak, the extent of the threat to public health and public safety, and the individual(s) responsible.

Activation

Once notified of a threat or disease outbreak that requires or potentially requires significant Federal public health and/or medical assistance, HHS convenes a meeting of the ESF #8 organizations and HHS Operating Divisions (e.g., CDC, the Food and Drug Administration, etc.) to assess the situation and determine the appropriate public health and medical actions. DHS coordinates all nonmedical support, discussions, and response actions.

The immediate task following any notification is to identify the population affected and at risk and the geographic scope of the incident. The initial public health and medical response includes some or all of the following actions:

- Targeted epidemiological investigation (e.g., contact tracing);
- Intensified surveillance within healthcare settings for patients with certain clinical signs and symptoms;
- Intensified collection and review of potentially related information (e.g., contacts with nurse call lines, laboratory test orders, school absences, and over-the-counter pharmacy sales); and
- Organization of Federal public health and medical response assets (in conjunction with State, local, and tribal officials) to include personnel, medical supplies, and materiel (e.g., the Strategic National Stockpile (SNS)).

Actions

Controlling the Epidemic

The following steps are required to contain and control an epidemic affecting large populations:

- HHS assists State, local, and tribal public health and medical authorities with epidemic surveillance and coordination.
- HHS assesses the need for increased surveillance in States or localities not initially involved in the outbreak and notifies the appropriate State and local public health officials with surveillance recommendations should increased surveillance in these localities be needed.
- DHS coordinates with HHS and State, local, and tribal officials on the messages released to the public to ensure that communications are consistent and accurate. Messages should address anxieties, alleviate any unwarranted concerns or distress, and enlist cooperation with necessary control measures. Public health and medical messages to the public should be communicated by a recognized health authority (e.g., the Surgeon General). (See the Public Affairs Support Annex.)

- If the outbreak first arises within the United States, HHS, in coordination with DOS, immediately notifies and coordinates with appropriate international health agencies such as the World Health Organization (WHO) and Pan American Health Organization as needed. Given the nature of many disease outbreaks, this notification and coordination may have occurred earlier in the process according to internal operating procedures. HHS advises the HSOC when notifications are made to international health agencies.

- The public health system, starting at the local level, is required to initiate appropriate protective and responsive measures for the affected population, including first responders and other workers engaged. These measures include mass vaccination or prophylaxis for populations at risk and populations not already exposed, but who are at risk of exposure from secondary transmission or the environment. An overarching goal is to develop, as early as possible in the management of a bioterrorism incident, a dynamic, prioritized list of treatment recommendations based on epidemiologic risk assessment and the biology of the disease/ microorganism in question, linked to the deployment of the SNS and communicated to the general public.

- HHS evaluates the event with its partner organizations and makes recommendations to the appropriate public health and medical authorities regarding the need for quarantine, shelter-in-place, or isolation to prevent the spread of disease. HHS coordinates closely with DHS regarding recommendations for medical needs that are met by NDMS and the U.S. Public Health Service Commissioned Corps.

- The Governor of an affected State implements isolation and/or social-distancing requirements using State/local legal authorities. In order to prevent the interstate spread of disease, HHS may take appropriate Federal actions using the authorities granted by U.S.C. title 42, 42 CFR parts 70 and 71, and 21 CFR 1240. State, local, and tribal assistance with the implementation and enforcement of isolation and/or quarantine actions is utilized if Federal authorities are invoked.

- Where the source of the epidemic has been identified as originating outside the United States, whether the result of terrorism or a natural outbreak, HHS works in a coordinated effort with DHS/Border and Transportation Security/Customs and Border Protection (DHS/BTS/CBP) to identify and isolate persons, cargo, mail, or conveyances entering the United States that may be contaminated. HHS provides information and training, as appropriate, to DHS/BTS/CBP personnel on identifying the biological hazard and employing "first responder" isolation protocols.

- The scope of the outbreak may require mass isolation or quarantine of affected or potentially affected persons. Depending on the type of event, food, animals, and other agricultural products may need to be quarantined to prevent further spread of disease. In this instance HHS and, as appropriate, the Department of Agriculture work with State, local, and tribal health and legal authorities to recommend the most feasible, effective, and legally enforceable methods of isolation and quarantine.

Decontamination

For certain types of biological incidents (e.g., anthrax), it may be necessary to assess the extent of contamination and decontaminate victims, responders, animals, equipment, buildings, critical infrastructure (e.g., subways, water utilities), and large outdoor areas. Such decontamination and related activities take place consistent with the roles and responsibilities, resources and capabilities, and procedures contained in the ESF #8 and ESF #10 Annexes, the Terrorism Incident Law Enforcement and Investigation Annex, and the Catastrophic Incident Annex. (Note: Currently no decontamination chemicals are registered (under the Federal Insecticide, Fungicide, and Rodenticide Act) for use on biological agents, and responders must request an emergency exemption from the EPA before chemicals can be used for biological decontamination.)

Special Issues

International Notification

A biological incident may involve internationally prescribed reportable diseases. In addition to case reporting, epidemics of disease with global public health significance must also be reported to international public health authorities.

Once a positive determination is made of an epidemic involving a contagious biological agent, HHS notifies DOS and DHS. HHS, in coordination with DOS, notifies the WHO and other international health agencies as appropriate.

Allocation and Rationing

If critical resources for protecting human life are insufficient to meet all domestic needs, the Secretary of HHS makes recommendations to the Secretary of Homeland Security regarding the allocation of scarce Federal public health and medical resources.

Responsibilities

The procedures in this annex are built on the core coordinating structures of the NRP. The responsibilities of each department and agency are described in the respective ESFs and Incident Annexes.

ENCLOSURE D

QUESTION 29

8/1/05 RESPONSE TO SENATOR LEAHY CONCERNING:

"Alerting Law Enforcement Officers to Terrorism Suspects Through VGTOF"

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

August 1, 2005

Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Leahy:

During the Senate Judiciary Committee's oversight hearing on July 27, 2005, you asked me to follow up on our discussion concerning the guidance provided to law enforcement officers when they encounter individuals who appear on a watchlist maintained by the Terrorist Screening Center. I appreciate this opportunity to respond to your request.

Attached is an explanation of the information provided to law enforcement officers when a check of the National Crime Information Center's database indicates that the subject has been entered in the Violent Gang and Terrorist Offender File (VGTOF). VGTOF provides the handling codes to which you referred during the hearing.

I appreciate your interest in this matter and your support for this and other FBI efforts. If you have additional questions, please do not hesitate to contact me.

Sincerely,

Robert S. Mueller, III
Director

Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Alerting Law Enforcement Officers to Terrorism Suspects Through VGTOF

When a law enforcement officer queries the National Crime Information Center (NCIC), several items of information may be obtained, including past offenses, sentences, and outstanding arrest warrants. This information may identify the person as armed and dangerous or may otherwise alert the officer to information important to the officer's safety.

The Violent Gang and Terrorist Organization File (VGTOF) is a component of NCIC. A subject is included in VGTOF if he or she is known or suspected to have engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (as provided in Homeland Security Presidential Directive (HSPD) 6 (9/16/03)) and certain identifying information is known to law enforcement officials, as discussed further below. Because all those associated with terrorism are potentially dangerous, all terrorism-related VGTOF entries are designated "Approach with Caution," regardless of whether the individual's terrorism-related activity has been violent. Unrelated to the individual threat that may be posed by a given VGTOF subject, all terrorism-related VGTOF entries receive one of four handling codes to reflect the nature and quality of the identifying information available on the subject and to identify the proper law enforcement response if the subject is encountered. As discussed further below, these codes are based on established criteria and are updated if warranted by new information. These handling codes are as follows.

Handling Code 1

Warning - Approach with Caution.

Arrest this individual. This individual is associated with terrorism. Once this individual is arrested, immediately contact the Terrorist Screening Center at (866) 872-9001 for additional information and direction.

If you are a Border Patrol Officer, immediately call the NTC [U.S. Customs and Border Protection's National Targeting Center].

Handling Code 2

Warning - Approach with Caution.

Please detain this individual for a reasonable amount of time for questioning. This individual is of investigative interest to law enforcement regarding association with terrorism. Immediately contact the Terrorist Screening Center at (866) 872-9001 for additional direction.

If you are a Border Patrol Officer, immediately contact the NTC.

Handling Code 3

Do Not Alert This Individual to This Notice.

The person queried through this search may be an individual identified by intelligence information as having possible ties with terrorism. Contact the Terrorist Screening Center at (866) 872-9001 for additional identifying information available to assist you in making this determination.

Do not arrest this individual unless there is evidence of a violation of federal, state, or local statutes. Conduct logical investigation using techniques authorized in your jurisdiction and ask probing questions to determine if this individual is identical to the person of law enforcement interest.

Warning - Approach with Caution.

If you are a Border Patrol Officer, immediately call the NTC.

Do Not Advise This Individual That They Are on a Terrorist Watchlist.

Handling Code 4

Do Not Alert This Individual to This Notice.

The person queried through this search may be an individual identified by intelligence information as having possible ties with

terrorism.

Contact the Terrorist Screening Center at (866) 872-9001 for additional identifying information that may be available to assist you in making this determination.

Do not arrest this individual unless there is evidence of a violation of federal, state, or local statutes. Attempt to obtain sufficient identification information to positively identify this individual in a manner consistent with the techniques authorized in your jurisdiction.

Warning - Approach with Caution.

If you are a Border Patrol Officer immediately call the NTC.

Do Not Advise This Individual That They Are on a Terrorist Watchlist.

All four handling codes indicate "Approach with Caution" because of the inherent danger in approaching a person known or suspected to have engaged in terrorist-related activity. The VGTOF handling code is not, however, designed to alert the law enforcement officer to the threat posed by the individual, since an individual's association with terrorism does not necessarily mean the individual is personally dangerous. While other NCIC information may alert the officer to a history of violent crimes, the VGTOF handling code itself does not provide this information. The VGTOF handling code instead relates to the amount and nature of the information available about the individual and, as additional information is obtained, a handling code may be revised to reflect that fact. For example, on 6/16/05 several thousand records were changed from Handling Code 4 to Handling Code 3 because full dates of birth or passport numbers were obtained. This migration from Handling Code 4 to Code 3 was the routine result of TSC's quality assurance process.

It is also important to understand how these handling codes are assigned. As a threshold matter, handling codes are assigned only to those included in VGTOF (as noted above, placement in VGTOF requires satisfaction of the criteria established by HSPD-6). The assignment of a VGTOF handling code is based on the following specific criteria.

- Among other things, the assignment of Handling Code 1 requires that there be a current, valid United States warrant or indictment for the subject, or an international arrest warrant or Interpol warrant accompanied by a corresponding warrant issued in the United States (such as a warrant for Unlawful Flight to Avoid Prosecution).

- The assignment of Handling Code 2 requires a reasonable, articulable suspicion of criminal domestic or international terrorism activity, a commitment from the Department of Homeland Security that they will issue a "Detainer" should the individual be encountered by law enforcement, or the presence of exigent circumstances. The determination that such a basis exists must be reviewed for legal sufficiency by the "nominating" office's Chief Division Counsel and the Office of the General Counsel at FBI Headquarters.

- Handling Code 3 is assigned to a person who has been placed in VGTOF consistent with HSPD-6 criteria where the subject's record contains the full first name, full last name, and either a complete date of birth or an accurate passport number, but does not meet the threshold for the assignment of Handling Code 1 or 2.

- Like Handling Code 3, Handling Code 4 is assigned to a person who has been placed in VGTOF consistent with HSPD-6 criteria, but only the subject's full first name and full last name are known, without the benefit of a complete date of birth or passport number.

As is apparent from the above instructions to law enforcement officers, all four handling codes request TSC notification. The program originally provided for Code 4 notifications to TSC only if the circumstances of the encounter were consistent with terrorist activity, because TSC was concerned that it would be unable to assist officers due to the very limited amount of information available as to Code 4 individuals. TSC was particularly concerned that if a law enforcement officer were to contact TSC with respect to numerous Code 4 subjects and received no assistance, the officer would stop contacting TSC not only in Code 4 cases but in Code 1, 2, and 3 cases as well, depriving both the officer and the TSC of valuable information.

This policy was changed in June 2005, and NCIC was asked to revise the instructions provided in Code 4 cases to request the same TSC notification requested for Codes 1, 2, and 3. This change was made based on the desire to capture as much intelligence information as possible by trying to make a positive identity match for all those encountered. NCIC has made the requested change, and law enforcement officers are now asked to notify TSC when a Code 4 individual is encountered. The effectiveness of this revision will be evaluated by TSC and efforts will continue to ensure the information provided to law enforcement officers is as complete and helpful as possible.

7/29/05

ENCLOSURE E

QUESTION 40

5/24/05 LETTER TO SENATE SELECT COMMITTEE ON INTELLIGENCE

U.S. Department of Justice

Office of Legislative Affairs

RECEIVED

2005 JUL -5 AM 11: 57

Office of the Assistant Attorney General — Washington, D.C. 20530

OIPR
DEPT OF JUSTICE

SECRET

MAY 24 2005

Senator Pat Roberts, Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Roberts:

I write to express the Department of Justice's strong opposition to any attempt to impose an "ascertainment" requirement on the implementation of multi-point or "roving" surveillance conducted under the Foreign Intelligence Surveillance Act (FISA). (U)

As the Members of this Committee are well aware, a roving surveillance order attaches to a particular target rather than to a particular phone or other communications facility. Since 1986, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering. Before the USA PATRIOT Act, however, FISA did not include a roving surveillance provision. Therefore, each time a suspect changed communication providers, investigators had to return to the FISA Court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap. However, international terrorists and spies are trained to thwart surveillance by regularly changing communication facilities, especially just prior to important meetings or communications. Therefore, without roving surveillance authority, investigators were often left two steps behind sophisticated terrorists and spies. (U)

Thankfully, section 206 of the USA PATRIOT Act ended this problem by providing national security investigators with the authority to obtain roving surveillance orders from the FISA Court. This provision has put investigators in a much better position to counter the actions of spies and terrorists who are trained to thwart

SECRET

Classified by: James A. Baker, Counsel for Intelligence Policy, Office of Intelligence Policy and Review, U.S. Department of Justice
Reason: 1.4(c)
Declassify on: X1

Declassified by James A. Baker
Counsel for Intelligence Policy
OIPR/USDOJ
Date: 7/9/05

surveillance. This is a tool that we do not use often, but when we use it, it is critical. As of March 30, 2005, it had been used 49 times and has proven effective in monitoring foreign powers and their agents. (U)

Some in Congress have expressed the view that an "ascertainment" requirement should be added to the provisions in FISA relating to "roving" surveillance authority. Section 2 of the S. 737, the Security and Freedom Ensured Act of 2005 ("SAFE Act"), for example, would provide that such surveillance may only be conducted when the presence of the target at a particular facility or place is "ascertained" by the person conducting the surveillance. (U)

Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA "roving" surveillance orders that pertains to "roving" wiretap orders issued in criminal investigations, but this is wholly inaccurate. The relevant provision of the criminal wiretap statute states that the roving interception of oral communications "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." *See* 18 U.S.C. § 2518(12). With respect to the roving interception of wire or electronic communications, however, the criminal wiretap statute imposes a more lenient standard, providing that surveillance can be conducted "only for such time as it is reasonable to presume that [the target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." *See* 18 U.S.C. § 2518(11)(b)(iv). (U)

Any "ascertainment" requirement, however, whether it is the one contained in the SAFE Act or the one currently contained in the criminal wiretap statute, should not be added to FISA. Any such requirement would deprive national security investigators of necessary flexibility in conducting sensitive surveillance. Due to the different ways in which foreign intelligence surveillance and criminal law enforcement surveillance are conducted as well as the heightened sophistication of terrorists and spies in avoiding detection, provisions from the criminal law cannot simply be imported wholesale into FISA. (U)

Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world. As a result, they generally engage in detailed and extensive counter-surveillance measures. Adding an ascertainment requirement to FISA therefore runs the risk of seriously jeopardizing the Department's ability to effectively conduct surveillance of these targets because, in attempting to comply with such a requirement, agents would run the risk of exposing themselves to sophisticated counter-surveillance efforts. (U)

In addition, an ascertainment requirement is unnecessary in light of the manner in which FISA surveillance is conducted. As the Members of this Committee are no doubt aware, intercepted communications under FISA are often not subject to contemporaneous monitoring but rather are later translated and culled pursuant to court-ordered minimization procedures. These procedures adequately protect the privacy concerns that we believe the proposed ascertainment provisions are intended in part to address. (U)

While we understand the concern that conversations of innocent Americans might be intercepted through roving surveillance under FISA, the Department does not believe that an ascertainment requirement is an appropriate mechanism for addressing this concern. Rather, we believe that the current safeguards contained in FISA along with those procedures required by the FISA Court amply protect the privacy of law-abiding Americans. (U)

First, under section 206, the target of roving surveillance must be identified or described in the order of the FISA Court, and if the target of the surveillance is only described, such description must be sufficiently specific to allow the FISA Court to find probable cause to believe that the specified target is a foreign power or agent of a foreign power. As a result, section 206 is always connected to a particular target of surveillance. Roving surveillance follows a specified target from phone to phone and does not "rove" from target to target. (U)

Second, surveillance under section 206 also can be ordered only after the FISA Court makes a finding that the actions of the specified target may have the effect of thwarting the surveillance (by thwarting the identification of those persons necessary to assist with the implementation of surveillance). (U)

Additionally, all "roving" surveillance orders under FISA must include Court-approved minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons. These are usually in the form of standard minimization procedures applicable to certain categories of surveillance, but the procedures may be modified in particular circumstances. (U)

(b)(1)1.4c

(b)(1)1.4c

In sum, the Department believes that the safeguards set forth in this letter reflect the appropriate balance between ensuring the effective surveillance of sophisticated foreign powers and their agents and protecting the privacy of the American people. The Department strongly opposes any attempt to disturb this balance by adding an ascertainment requirement to the provisions of FISA relating to roving surveillance authority. (U)

We hope that this information will be useful to the Committee as it considers the reauthorization of those USA PATRIOT Act provisions scheduled to sunset at the end of this year. Please do not hesitate to contact me if you have additional questions or concerns about this issue. (U)

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General