FBI Director Robert S. Mueller, III
Responses to Questions for the Record
From Senator John D. Rockefeller IV

1. **In his recent State of the Union speech, President Bush announced that he has instructed the Director of Central Intelligence, the Director of the FBI, working with the Attorney General, and the Secretaries of Homeland Security and Defense to develop a Terrorist Threat Integration Center (TTIC). This new center will merge and analyze terrorist-related information collected domestically and abroad in order to form the most comprehensive possible threat picture. Please elaborate on how this new Center will function.**

(A) How will it be managed, and what, if any, limitations will be put on the intelligence to be shared?

Response:

The TTIC is a joint venture between the participating agencies. It is managed by a Director selected by the Director of Central Intelligence in consultation with the Secretaries of Homeland Security, Defense, the Attorney General and the Director of the FBI. The TTIC will also have one Principal Deputy Director from an agency different than the Director of TTIC.

The TTIC Director will supervise and manage the all-source analysis of terrorist threat information done in the TTIC. He will not direct operations. The TTIC will have access to all terrorist threat information available to the U.S. Government. The TTIC will be a significant contributor to the development of requirements for intelligence collection, but the fulfillment of those requirements will be conducted by the operational arms of the relevant agencies under their existing authorities and command structure.

The operational bodies of the FBI and CIA will retain all of their existing authorities (and limitations), reporting structures, and chains of command. There will be no operational changes brought about by the co-location -- other than the fact that coordination and communication will be simplified by virtue of being located in the same facility. The respective operational divisions will not be under the direction of the TTIC Director. The TTIC is strictly analytic in nature.

(B) When do you anticipate that this Center will be fully operational as envisioned?

Response:

The final stage of TTIC implementation will occur when the new facility is ready which

is expected approximately Summer 2004.

(C) What additional resources will be needed to fund the FBI's contribution to this Center?

Response:

TTIC is building a proposed budget to cover the creation of an IT architecture that will, at a minimum, support TTIC requirements and may support the requirements of both the FBI's Counterterrorism Division (CTD) and the CIA's Counterterrorism Center (CTC). To what degree either FBI or CIA contribute to this effort remains unresolved.

(D) Is there also a plan to move the Counterterrorism Division of the FBI and the DCI's Counterterrorism Center (CTC) into one building?

Response:

The final stage of TTIC implementation includes the co-location of substantial elements of the FBI's CTD and the CIA's CTC. The co-location effort will take place at a neutral site away from either CIA or FBI headquarters. Locating the TTIC in the same facility as the primary operational arms of the CIA and FBI is beneficial in that the analysts will be closer to the gatherers of the information which has been proven to enhance both the quality of analysis and the effectiveness of investigations.

(E) To what extent were you consulted about the formation of this Center prior to the President's State of the Union speech?

Response:

The FBI, the Director of Central Intelligence, and other Intelligence Community officials engaged in discussions with the Administration about the formation of an intelligence fusion center prior to the President's State of the Union speech.

2. **The recent "Slammer" computer virus, which struck thousands of computers, crashing bank machines and disrupting businesses and Internet connections, underscores the vulnerability of the U.S. economy to cyberterrorism.**

(A) Do we have any information that al-Qaida has the interest or ability to conduct cyberterrorist operations against the U.S.?

Response:

Al-Qaeda has demonstrated a capability to carry out innovative, complex, and simultaneous attacks such as September 11, 2001 and the 1998 bombings of the U.S. embassies in Kenya and Tanzania. Although unlikely to abandon its principal means of attack, bombings and small arms, al-Qaeda's ability to plan and initiate innovative attacks indicates that the group may be receptive to new methods of attack, including cyber, as part of a compound physical and cyber attack. Currently, al-Qaeda has not displayed a computer network attack (CNA) capability. However, the group uses computers to communicate, plan, gather information on potential targets, and acquire logistical support. The recent geographical dispersion of al-Qaeda personnel by U.S. military actions may cause an increase in the group's use of the Internet for communication and coordination.

In addition, the increased attention focused on the group by law enforcement and intelligence agencies worldwide, as well as new security measures in place at potential U.S. targets, may lead al-Qaeda to increase its information technology sophistication in order to bypass new defensive measures. This might include:

- Seeking insiders with cyber access to potential target sets
- Recruiting computer experts or students with computer expertise
- Employing an unwitting computer expert
- Developing or using tools, devices, and malicious software to access and attack targets.

As with many groups, al-Qaeda reviews its past successes and failures. The impact of the September 11 attacks on the World Trade Center and the Pentagon may induce them to look further at vulnerabilities in U.S. critical infrastructure (e.g., banking, telecommunications, electric power, etc.) and the potential damage and disruption that could result from an attack, whether direct or indirect, on a portion of that infrastructure. Other terrorist groups, particularly militant Islamic groups, are also aware of the potential economic and social effects of attacking infrastructure. Many of these groups maintain ties to other groups, including al-Qaeda. These connections could result in "proxy" groups conducting attacks in support of al-Qaeda or the various groups exchanging targeting information on sectors of the U.S. infrastructure.

(B) What terrorist groups are the likeliest to conduct such operations?

Response:

Terrorist groups have not yet displayed a proven capability in CNA. There are a number of reasons why terrorists have not pursued this more aggressively, including a historical preference for physical attacks over more sophisticated but less visible attacks, and the tendency to rely on members' expertise rather than to consult outside professionals. Even so, some terrorist groups may have understood the significance of the effects of the

September 11 attacks on the nation's infrastructure and look to repeat and broaden those effects in future attacks.

(C) What is the ability of the U.S. Intelligence Community to provide actionable warning of cyber attacks?

Response:

The ability to provide information on emerging capabilities and potential threats is an interagency effort that takes into account signals intelligence and human intelligence, as well as information from open sources, including academic and private organizations that monitor vulnerabilities, exploits, and malicious code such as viruses, worms, and denial-of-service attacks. It is difficult to assess current capability given the lack of traditional indicators combined with the voluminous non-terrorist related cyber incidents.

The indicators of a CNA program differ from any other. Conventional military strength, for example, is easily detected and assessed. Nations must either purchase weapons systems or have the industrial capacity to build them. Moreover, the more powerful the weapon system (e.g., tanks, aircraft, and naval vessels), the easier it is to detect. CNA programs, however, also differ from other non-conventional weapons programs. CNA programs do not require the detectable engineering research, development, testing, and evaluation that complex weapon platforms such as ballistic missiles require. They do not require the concentration of highly specialized knowledge (or the program signatures) that nuclear, biological, or chemical weapons programs do. Funding a CNA program can be done clandestinely and, with direction, it can be masked as legitimate businesses or research and development.

(D) To the extent that this is a problem area, what is being done to rectify it?

Response:

The FBI has undergone significant changes, including the reorganization of resources to more appropriately address terrorism and the creation of the Cyber Division (CyD). By creating the CyD, the FBI has reorganized investigative resources to more effectively address the emerging cyber threat that our country faces, including, in priority order, cyber-terrorism, cyber-counterintelligence and cyber-crime.

The mission of the CyD is to: (1) coordinate, supervise and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist organizations, foreign government sponsored intelligence operations, or criminal activity and for which the use of such systems is essential to that activity; and (2) form and maintain public/private alliances in conjunction with enhanced education and training to maximize

counterterrorism, counterintelligence, and law enforcement cyber response capabilities.

The key to protecting our National Information Infrastructure from a cyber attack is information, which serves as the foundation of an effective intelligence base. It is realized that the government, including the FBI, must work better with the private sector and government partners to facilitate a meaningful information exchange focused on actual cyber threats.

The FBI has formed an Interagency Coordination Cell (IACC) which holds monthly meetings regarding ongoing investigations with pertinent government agencies. This entity is currently operating under and supported by the Cyber Division Computer Intrusion Section and its membership has risen to approximately 35 government agencies that meet on a monthly basis, and as needed, to address specific threats and vulnerabilities. The IACC includes representation from NASA , U.S. Postal Service, Air Force Office of Special Investigations, U.S. Secret Service, U.S. Customs, Departments of Energy, State and Education, and the CIA, to name a few.

The IACC's accomplishments to date include the formation of several joint investigative task forces with member agencies participating, and over 30 separate instances of joint investigations being initiated as a direct result of IACC meetings, information sharing and participation. In one case, an IACC member agency provided timely sensitive source information to the appropriate authorities which prevented the planned intrusion and compromise of another government agency's computer system and the preservation of critical log data used for the ensuing investigation.

The IACC's members are currently working on the establishment and development of a database which would serve as a source of computer intrusion information compiled from member agency investigations to facilitate other investigations. It is also working on the establishment and administration of a dedicated virtual private secure network for member agencies to communicate vital infrastructure protection and computer intrusion information for immediate emergency response situations, in addition to dissemination of routine but sensitive information.

(E) How does the transfer of the National Infrastructure Protection Center (NIPC) into the Homeland Security Department affect the government's approach to this problem?

Response:

The ability of the U.S. Intelligence Community to provide actionable warning of cyber attacks, was discussed in an April, 2001 General Accounting Office Report, which listed strategic analysis (including advance warning of cyber attacks) as one of the NIPC's challenges. NIPC's mission and challenges were transferred to the Department of

Homeland Security (DHS) in March 2003. Although the mission and many key personnel have been transferred to DHS, the FBI will continue work closely with the new Department, sharing threat information to assist in risk assessments. The FBI has provided several liaison personnel to DHS, and NIPC personnel and functions continue to be located within FBI spaces.

It is our understanding that DHS, through the Directorate of Information Analysis and Infrastructure Protection (IAIP) will merge under one roof the capability to identify and assess current and future threats to the homeland, map those against our vulnerabilities, issue timely warnings and take preventive and protective action. Regarding cyber attacks, the IAIP Directorate places an especially high priority on protecting our cyber infrastructure from terrorist attack by unifying and focusing the key cyber security activities performed by the Critical Infrastructure Assurance Office and the National Infrastructure Protection Center.

3. **The potential use of terrorism against agricultural targets (i.e., agroterrorism) raises the prospects of significant economic loss and market disruption. U.S. Department of Agriculture officials estimate that a single agroterrorist attack on the livestock industry using a highly infective agent, for example, could cost the U.S. economy between $10 billion and $30 billion.**

(A) How great do you consider the threat of agroterrorism to the U.S.?

Response:

Although we are unaware of any specific threats, the FBI considers the U.S. agricultural industry vulnerable to terrorism based on the following facts:

Accessibility: Biological agents that have significant impact on crops and livestock exist around the world, both naturally and artificially maintained in veterinary laboratories. Most notably, the recent Foot and Mouth Disease (FMD) epidemic in the United Kingdom had a devastating impact on the U.K.'s agriculture industry resulting in the loss of large amounts of money as well as a food source. The locations of the outbreaks of the disease were well publicized, and could have been used to determine where to get a virulent form of the virus. Also, the vast open spaces that are a hallmark of agriculture are largely unprotected against potential terrorists, and therefore seem to be extremely susceptible to an act of biological terrorism.

Means of Production: In order to produce large quantities of biological agents of agricultural concern, a person must have the materials, equipment and knowledge to grow the agents in large quantities. Some biological agents,

such as viruses (*e.g.*, FMD virus) require special materials (such as animal cell cultures), equipment and specialized training. However, other biological agents, such as bacteria (*e.g.* the causative agent of Anthrax), are easier to grow and require simpler equipment and training.

While being able to produce large quantities of bacteria or virus may be desirable for someone to commit an act of agricultural bioterrorism, it is not essential for some biological agents. In fact, a person without the materials, equipment or technical knowledge could still successfully create an agricultural epidemic.

Operational Practicality: One of the major obstacles for producing a biological agent to target a human population is preparing the material in a way that it is respirable for a susceptible person. Producing a biological aerosol would allow for a person to have a maximum effect without the intended target(s) knowing that they were attacked. For example, a person sprayed with a liquid or injected with a needle full of a biological pathogen, might suspect that they may be in danger. However, direct exposure or injection of plants or animals remain realistic means by which these "victims" may become exposed.

Preparedness: In contrast to the U.S. public health's preparedness for response to biological terrorism, the agricultural and veterinary community is less effective in its ability to detect and respond to an act of agricultural bioterrorism.

However, the threat to U.S. agriculture may be less than the vulnerability would suggest due to certain conditions, including: (1) diffuse nature of the target; (2) the time between launching an attack and seeing the effects; and (3) the interests of terrorists to launch other types of attacks that kill or injure humans rather than those that effect an infrastructure, such as agriculture.

(B) Do you have any information that terrorists or terrorist groups have tried to target U.S. agriculture?

Response:

Historically, there are examples of agroterrorism. The Ethiopian calendar still celebrates a day memorializing a late 19th century attack by Italian government interests against the Ethiopian cattle industry with the pathogen "Rinderpest" (not pathogenic toward humans).

During World War I, agents of the German government launched several attacks with the causative agents of anthrax and glanders (the latter is a debilitating disease of quadrupeds). These attacks were launched in Norway (against reindeer herds, thought to be used by the British to carry supplies in northern Norway); Argentina; Persia; and the US. The attacks in Persia (now Iraq and Iran) were successful, causing the British forces to halt their advance in the Mesopotamian desert owing to a lack of supply animals (horses, mules and camels, which were sickened with glanders).

No one knows whether the US attacks -- launched by agents of the German government out of Washington and conducted in Baltimore, New York, and St. Louis -- were successful, because no one was monitoring for such attacks. The attacks occurred in 1914-1915, during the period when the US was officially neutral in the European conflict (WWI). The attacks came to light in testimony obtained during hearings into the disposition of alien property seized by the US pursuant to our declaration of war. The investigation was headed by John McCoy (later the Secretary of the Army and Deputy Director of the CIA) and lasted from 1920 - 1943 when the state of war with Germany and Austria made the judgement moot.

(C) What are you doing to increase awareness of this threat within the United States?

Response:

The FBI is addressing the awareness of potential attacks on livestock, crop, and food through efforts intended to share potential threat information and intelligence on four levels:

(1) Through national level liaisons that have been established with: the US Department of Agriculture; the Food and Drug Administration; the Department of Health and Human Services/Centers for Disease Control; and the US Intelligence Community.

(2) Through liaisons established with local, county, and state officials, as well as regional federal partners by the FBI field office Joint Terrorism Task Forces. Currently, there are 66 FBI JTTFs nationwide.

(3) Law enforcement sensitive information/intelligence is also communicated to the nation's law enforcement community through the National Law Enforcement Telecommunications System (NLETS) and FBI generated intelligence reports to the intelligence community.

(4) The FBI is working closely with DHS to directly inform key infrastructures of potential threats at both the national and local regional levels.

4. **Late last year, the House and Senate intelligence oversight committees released the findings, conclusions and recommendations of the Joint Inquiry into the terrorist attacks of September 11, 2001. The Joint Inquiry also expressed concern with the reorientation of the FBI to counterterrorism and suggested consideration of the creation of a new domestic surveillance agency similar to Great Britain's MI5.**

(A) What is your opinion about the pros and cons of creating a new domestic surveillance agency?

Response:

For nearly 100 years, the FBI has earned a reputation as the world's premier law enforcement agency based primarily on its ability to collect information - whether through physical surveillance, electronic surveillance or human source development. For these reasons, the FBI is in the best position to continue to serve as the primary domestic intelligence service for the United States government.

The FBI's ability to pursue an investigation through both traditional law enforcement means and through intelligence collection and operations is a tremendous asset in the war against terrorism. As demonstrated by a number of the international terrorism investigations since 9/11 that have employed prosecutions as one tool to prevent terrorism, such as the arrest and neutralization of the terrorist cell in Lackawanna, New York, the combination of intelligence and prosecutorial functions is a potent and critical ingredient of our anti-terrorism approach. Close coordination of all available tools in the fight against terrorism -- intelligence, military, diplomatic, and law enforcement -- enables strategic application of the best combination of efforts in any particular situation to disrupt terrorist activity. That coordination -- which is now greatly facilitated by the November 18, 2002 FISA Court of Review decision -- is essential to a successful strategic effort against terrorism, and is best achieved by retaining the domestic intelligence and criminal investigative responsibilities within one agency.

(B) What can we learn from Great Britain's experience with MI5?

Response:

We believe that the experience in Great Britain and in many democratic nations which have independent intelligence and law enforcement agencies highlights the inherent difficulties engendered by a lack of coordination between these two critical functions.

5. **(A) To what extent has your organization committed to providing intelligence analysts and other staff to the new Department of Homeland Security?**

Response:

With the creation of DHS, the FBI transferred both Agent and support personnel positions to the DHS. (see detail in response to (B), below). The FBI is currently providing general administrative support to the DHS as detailed in the current Memorandum of Understanding entered into by the Department of Justice and the DHS that runs through the end of FY 2003.

(B) How many employees have you committed, or anticipate committing, to the new Department?

Response:

The creation of DHS required the FBI to transfer 129 agent positions and 87 support personnel positions assigned to the Critical Asset Program and National Infrastructure Protection Program to the DHS. The FBI also has assigned seven counterterrorism agents to the DHS in the following positions: Director of Intelligence Fusion; Director for Domestic Threat, Intelligence, and Detection; Liaison Officer (LNO) to the Threat Countermeasures and Incident Management Directorate; and three remaining LNOs assigned to the Threat Monitoring Center, Response and Recovery Directorate, and Protection and Prevention Directorate.

In addition to the seven agents detailed above, the FBI is also in receipt of a DHS request, dated April 15, 2003, for two additional FBI support positions specific to infrastructure protection.

The FBI will continue to provide general administrative support to the DHS as detailed in the current Memorandum of Understanding entered into by the Department of Justice and the DHS that runs through the end of FY 2003.

(C) For how long will these employees be on loan to the Department?

Response:

The FBI and the DHS are working together to assess the level of support the DHS requires from the FBI. This assessment will determine the length of time that the seven FBI agents are detailed to the DHS. Additionally, the two support positions are proposed for a period of one year.

FBI personnel that are providing general administrative support to DHS, but are not officially on loan, are covered by the current Memorandum of Understanding entered into by the Department of Justice and DHS that runs through the end of FY 2003. This agreement may be extended by mutual written agreement of both parties. In addition, either party, upon 60 days written notice to the other party, may terminate this agreement.

(D) Have you determined the categories of information that you will be providing to the Department of Homeland Security without a specific request from Secretary Ridge? If so, what are they?

Response:

DHS receives a wide range of FBI information in a variety of different formats. The following are examples of information that is provided to DHS without a specific request from Secretary Ridge.

- All products distributed to the law enforcement community via the National Law Enforcement Telecommunications System (NLETS) to include products of the Homeland Security Advisory System. These reports are produced as needed in an unclassified format.

- The FBI Intelligence Bulletin. This report is produced weekly in an unclassified format.

- The CT-Watch Update. This report is produced daily in a classified format.

- Terrorism Reports and Requirements Section (TRRS), Intelligence Information Reports (IIGS). These TRRS reports are raw reports distributed to the Intelligence Community (IC). These reports are produced as needed in both an unclassified and classified format.

(E) How will your commitment to the Department of Homeland Security diminish your ability to focus on other Intelligence Community priorities?

Response:

The current level of committed resources does not have a negative impact on the FBI's ability to focus on other IC priorities. Rather, it is anticipated that increased information sharing with the DHS will sharpen the FBI's focus on IC priorities.

It should further be noted that in an effort to enhance information sharing at all levels, DHS has established two full-time liaison officers within the FBI. One of these liaison officers functions as the "Senior Representative." The second liaison officer functions as the DHS representative to CT-Watch. Furthermore, DHS has been formally invited to increase its representation within the CT-Watch to a level appropriate with its needs, as well as fill the role of deputy within the National Joint Terrorism Task Force (NJTTF).

6. **Suspected Hizballah members in the U.S. are believed to be primarily engaged in fund raising on behalf of the group's activities overseas. Hizballah members in the U.S. have also engaged in criminal activities, such as narcotics trafficking and cigarette smuggling, to raise funds for the group.**

(A) Under what circumstances do you consider it likely that Hizballah will conduct terrorist activity inside the U.S.?

Response:

It is our judgment that Hizballah would consider terrorist attacks in the United States only as a last resort, and then only in response to US military action against the group in Lebanon or a US war with Iran. Hizballah is unlikely to risk the certain and significant US countermeasures against Hizballah that would follow an attack in the US homeland, especially given the group's demonstrated ability to target Western interests overseas. Hizballah's public relations apparatus has been working aggressively since 9/11 to forestall further US Government pressure on the group in order to maintain its current stature in the political arena in Lebanon.

(B) How would Hizballah – both domestically and internationally – react to U.S. military operations against Iraq?

Response:

Hizballah, a Shia extremist group with close ties to the Government of Iran, has consistently opposed the US military presence in the Middle East at large and recently in Iraq. Recent press reporting indicates that Lebanese Hizballah members are present in Iraq, however the intent and activities of these individuals remains unclear. An article in the Los Angeles Times on 4/17/03 quoted Hizballah's Secretary General

Hassan Nasrallah as saying "The people of the region will receive [America] with rifles, blood, arms, martyrdom and martyrdom operations."

That statement, while threatening, did not specifically state that Hizballah would perpetrate attacks against the US and was, therefore, in keeping with Hizballah's other public statements on the US war in Iraq. Hizballah appeared to be attempting to walk a fine line, on the one hand maintaining its jihadi image with sharply worded anti-American vitriol, while on the other hand seeking to avoid becoming a target itself of more direct US pressure or action. As we have now seen, Hizballah did not engage coalition forces through terrorism.

7. **It has been reported in the press that Libya has been sending signals that it wants to get out of the terrorism business and has offered to compensate the families of the victims of the bombing of Pan Am Flight 103. Sudan has reportedly arrested al-Qaida members and "by and large" shut down al-Qaida training camps on its territory.**

(A) To what extent, if any, have Sudan and Libya diminished their support for terrorism? If so, how has that manifested itself?

Response:

We are not aware of current active involvement of the Government of Libya in international terrorism, but Libya continues to harbor suspects in the 1989 bombing of French UTA Flight 772, which killed 171 passengers including seven U.S. citizens. Libya also continues to harbor suspects in the 1986 bombing of LaBelle Disco in Berlin, which killed three (including two U.S. servicemen) and wounded more than one hundred (including 56 U.S. citizens).

As with Pan Am 103, Libya denies any responsibility for these attacks. Libya is purported to have paid reparations to the French government with respect to the UTA bombing, but we have no information regarding admissions of liability.

We are not aware of current active involvement of the Government of Sudan in international terrorism, but Sudan remains a permissive environment and a transit point for Islamic extremists who engage in recruiting, training, fundraising, and logistical support for terrorist activity worldwide.

(B) To what extent, if any, are these nations assisting in the War on Terrorism?

Response:

From our perspective any appearance of cooperation by Qadhafi with the War on Terrorism reflects successful perception management rather than genuine commitment.

We have no relationship with Libyan intelligence services. Despite its much belabored extradition of two intelligence officers for trial in the Netherlands, Libya continues to deny responsibility for the 1988 bombing of Pan Am 103.

From our perspective, Sudan's cooperation with the War on Terrorism is begrudging at best -- designed to curry favor with the US Government, but in actuality neither genuine nor particularly effective.

Sudan's cooperation with FBI investigations has been fitful. Sudan has detained certain individuals at our request but thereafter has denied our access to them or delayed such access for years. Sudan has also denied or delayed for years our access to certain documents and materials confiscated from such individuals. Other individuals detained by Sudan of its own accord and to whom we are provided access have little relevant information to offer.

There have been instances where Sudan has ceded to us access to individuals and materials, which are of benefit to our investigations, but on the whole Sudan creates the appearance of cooperation more readily than it cooperates.

8. **In 1996, the Committee was informed by the CIA that "[w]e see government-orchestrated theft of U.S. corporated S&T [science and technology] data as the type of espionage that poses the greatest threat to U.S. economic competitiveness. We have only identified about a half dozen governments that we believe have extensively engaged in economic espionage as we define it. These governments include France, Israel, China, Russia, Iran and Cuba."**

(A) What new trends do you see in the economic espionage threat to the U.S.?

Response:

The FBI has identified several recent trends in the area of economic intelligence collection. FBI investigations indicate that the traditional collectors of U.S. economic and proprietary information are expanding their list of priority targets and increasing their official and non-official presence in the United States. Priority sectors being targeted by these foreign powers include:

- US national defense and trade information;
- Aerospace technologies;

- Computer technologies (especially nano-technologies);
- Telecommunications;
- Biotechnology; and
- Data technology.

In addition, the FBI has noted the increased targeting by some countries of academic and special interest groups in the United States. This type of spotting, accessing and targeting avoids direct approaches which could reveal intelligence activities. Finally, the increasing amount of travel by U.S. delegations to other countries offers foreign intelligence services more opportunities to spot, assess, cultivate, pitch, and recruit such U.S. persons.

(B) What does the U.S. government do to alert U.S. industry to these threats?

Response:

The Awareness of National Issues Response (ANSIR) Program is currently the FBI's most useful tool for raising awareness of U.S. industry concerning Economic Espionage threats. The ANSIR program is an officially sanctioned outreach program that interacts with industry.

ANSIR originally focused on companies doing work for the government at the classified level. In the defense industrial base (300,000 companies), for instance, there are approximately 11,000 companies that are considered "secure contractors." The FBI has, however, expanded the ANSIR program to embrace more of the private sector, since many of the threats have turned their attention to stealing trade secrets. The FBI posts one ANSIR Coordinator in each field office. That individual, who is also an FBI Special Agent, is assigned to work with local companies on all counterintelligence threats. The large amount of the ANSIR coordinator's efforts are spent addressing trade secret theft and the economic espionage component.