S. HRG. 107–971

REFORMING THE FBI IN THE 21ST CENTURY

HEARINGS

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MARCH 21, APRIL 9, AND MAY 8, 2002

Serial No. J–107–69

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

88–571 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
MARIA CANTWELL, Washington
JOHN EDWARDS, North Carolina

ORRIN G. HATCH, Utah
STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
SAM BROWNBACK, Kansas
MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

CONTENTS

THURSDAY, MARCH 21, 2002

STATEMENTS OF COMMITTEE MEMBERS

Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa 22
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah 4
prepared statement 52
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 1
prepared statement 54
Sessions, Hon. Jeff, a U.S. Senator from the State of Alabama 18

WITNESSES

Chiaradio, Robert J., Executive Assistant Director for Administration, Federal Bureau of Investigation, Department of Justice, Washington, D.C.; accompanied by Bob Dies, Chief Technology Officer, Federal Bureau of Investigation, and Bill Hooten, Assistant Director for Records Management, Federal Bureau of Investigation 9
Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C. .. 6

SUBMISSIONS FOR THE RECORD

Chiaradio, Robert J., Executive Assistant Director for Administration, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement 28
Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C., prepared statement 36
Mueller, Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C., statement 57

TUESDAY, APRIL 9, 2002

STATEMENTS OF COMMITTEE MEMBERS

DeWine, Hon. Mike, a U.S. Senator from the State of Ohio 64
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois 75
Grassley, Hon. Charles E., a U.S. Senator from the State of Iowa 64
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah 66
prepared statement 105
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 61
prepared statement 107

WITNESSES

Senser, Kenneth H., Assistant Director, Security Division, Federal Bureau of Investigation, Department of Justice, Washington, D.C. 89
Szady, David, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Department of Justice, Washington, D.C. 86
Watson, Dale, Executive Assistant Director for Counterterrorism/ Counterintelligence, Federal Bureau of Investigation, Department of Justice, Washington, D.C. 91
Webster, William H., Milbank, Tweed, Hadley and McCoy, LLP, Washington, D.C. 65

Page

QUESTIONS AND ANSWERS

Responses of Kenneth Senser to questions submitted by Senator Grassley 100

SUBMISSIONS FOR THE RECORD

Senser, Kenneth H., Assistant Director, Security Division, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement 113
Szady, David, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement 125
Webster, William H., Milbank, Tweed, Hadley and McCoy, LLP, Washington, D.C., prepared statement and attachment 130

WEDNESDAY, MAY 8, 2002

STATEMENTS OF COMMITTEE MEMBERS

Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah, prepared statement 241
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 135
prepared statement 243
Thurmond, Hon. Strom, a U.S. Senator from the State of South Carolina, prepared statement 265

WITNESSES

Mueller, Hon. Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C. 139
Thompson, Hon. Larry D., Deputy Attorney General, Department of Justice, Washington, D.C. 137

QUESTIONS AND ANSWERS

Response of the Department of Justice to a question submitted by Senator Leahy (December 23, 2002) 172
Responses of the Department of Justice to questions submitted by Senators Leahy and Feingold (April 11, 2003) 175
Responses of the Department of Justice to questions submitted by Senators Leahy and Feingold (July 10, 2003) 206
Responses of the Department of Justice to questions submitted by Senator Leahy (July 17, 2003) 238

SUBMISSIONS FOR THE RECORD

Mueller, Hon. Robert S., III, Director, Federal Bureau of Investigation, Department of Justice, Washington, D.C., prepared statement 248
Thompson, Hon. Larry D., Deputy Attorney General, Department of Justice, Washington, D.C., prepared statement 258

REFORMING THE FBI IN THE 21ST CENTURY: LESSONS FROM THE OKLAHOMA CITY BOMBING CASE

THURSDAY, MARCH 21, 2002

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, Pursuant to notice, at 9:34 a.m., in room SD–106, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Hatch, Grassley, Specter, and Sessions.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning. Please, all the witnesses come up and take a seat. I want to thank the witnesses from the FBI for their cooperation in agreeing that everybody will sit at the table.

We have this situation where the Republican Leader, exercising his rights under the rules, has objected to any committees being more than 2 hours into the session. But this is an extremely important issue, one that the American people and the FBI are quite concerned about, how we deal with the FBI's readiness to meet the law enforcement challenges of not only today but of tomorrow, too.

We began oversight hearings last summer, and I think this is extremely important because the FBI is facing some unprecedented challenges. Also, under the new legislation we passed, they have unprecedented powers and we want to make sure in a democratic society that we balance those. We also want to make sure that the FBI is able to do all the things necessary to protect this great Nation.

It is the committee's responsibility to ensure that the FBI is as great as it can be, and this series of oversight hearings is a fundamental part of that. We will consider the FBI's production, and it was actually belated production, as the important and thorough report by the Inspector General revealed this week, of the Oklahoma City documents. Also, we will look at the question of the destruction of some of them.

What is troubling to me in that report, actually more troubling than the belated production or the destruction, is the conclusion that senior FBI personnel failed to notify either the prosecutors on the case or high-ranking Justice Department officials, including the current FBI Director, Robert Mueller, who was then serving as the

Acting Deputy Attorney General, about the belated document production problems until 1 week before the scheduled execution date for Timothy McVeigh.

I am concerned about that because the trial had been a textbook trial of how to do things right on both the prosecution side and the defense side. After the millions of dollars spent on that trial, to suddenly find a glitch like this that could have derailed the whole process is very troubling.

The Inspector General's report revealed that the destruction of relevant FBI documents was not disclosed to the court or the prosecutors on the case or the defense until after Timothy McVeigh's execution. I agree with the conclusion in the Inspector General's report that the court and defense counsel should have been informed of the FBI's destruction of documents, in addition to being given the belated documents, while McVeigh's stay of execution was being litigated. It is unlikely that any of the destroyed documents, if produced, would have changed the outcome of the case, but that does not excuse the FBI's conduct.

The observations of the presiding judge in the case are illuminating. He described the FBI as "an undisciplined organization or organization that is not adequately controlled or that can't keep track of its information." In denying the request for a stay of execution, he noted "It is the function others to hold the FBI accountable for its conduct here, as elsewhere."

The report raises three significant issues for this committee's review, as we are one of the ones that the court meant should look into this. First, there are structural and management problems at the FBI which need fixing. You can't blame a computer or filing system when senior FBI agents in charge of the Oklahoma City bombing case are aware of document production problems almost 5 months before the scheduled execution.

FBI headquarters officials were aware nearly 3 months before the scheduled execution, but did not disclose these problems to the FBI director, to senior Justice Department officers, or to prosecutors on the case until a week before the scheduled execution. It is hard to blame those who are in charge when they don't get the information.

I am afraid it is an example of a "circle the wagons" mentality. If you learn about a problem, you can't bury your head in the sand and hope it goes away. And you can't contain a problem under the cloak of secrecy; it just aggravates it.

We will look to Director Mueller to consider appropriate administrative action against the FBI managers who did not promptly tell FBI headquarters or Justice Department officials. But the silver lining in the Inspector General's report is the conduct of two lower-level employees who, in contrast to the managers, did the right thing.

The FBI financial analyst and the intelligence research specialist who first discovered the document production problem in January 2001 informed their superiors in the chain of command, but did not go around them. As the report notes, "the FBI could do well to use this as an opportunity to help remedy a longstanding FBI problem—the belief among FBI employees that bringing problems to management's attention only results in problems for the employee."

Second, the information management and technology problems at the FBI substantially contributed to the belated document production. We are all relieved that the Inspector General found no intentional misconduct, but the report documents a number of fundamental flaws in the handling of information by the FBI that contributed to the failure to produce documents in the Oklahoma City bombing case: "antiquated and inefficient computer systems;" "inattention to information management;" "inadequate quality control systems;" misfiling, mislaying or losing documents; failure by field offices to follow correct procedures. The litany of problems is startling and that is why I want to hear from the FBI what is going to happen on this. Mr. Dies, I am glad you are here on that.

I appreciate, and I think most members on this committee appreciate the efforts of the director to correct the management and information management problems at the FBI. I hope he appreciates the fact that congressional involvement can help achieve that.

In the Emergency Supplemental Appropriations Act passed in January, Congress, with my support, gave the FBI $745 million, with more than $417 of that dedicated to computer and information technology. We are poised to give another $245 million. That would amount to $1 billion infusion of funds into the FBI, or a 25-percent budget increase since September 11.

Now, we are giving more powers, we are giving more money, but the quid pro quo is that the problems will be fixed. This committee cannot authorize more money, will not authorize more money, nor will the Appropriations Committee appropriate it if the problems are not being fixed.

Finally, we have to apply the lessons of Oklahoma City to the challenges facing the FBI in fighting terrorism because Oklahoma City, the problems there, the problems before September 11, can be problems today, on March 21. There is nobody in this room who would ever assume that we have seen our last domestic terrorism or international terrorism attack within the shores of the United States. We are sitting in a building that is just yards away from one of the buildings probably targeted in the September 11 attacks. So we have to look at this.

There are parts of the Inspector General's report that are chilling. They raise the critical question of whether the same flaws hampered the FBI's sharing of counter-terrorism information before the September 11 terrorist attacks.

I know there are some in the Congress who don't want us to look into the question of whether mistakes were made prior to September 11. I would say that those feelings are not shared by the heads of the FBI, Director Mueller and others. They have been very open with me that we will look at the problems of sharing information.

Right now, it is fair to conclude that the FBI does not know what it knows. That is the problem. You have got all this information, but if you can't know what you know, it is not going to help us. If the information is sitting locked up somewhere, it is not going to help. If it is material that hasn't been translated, it is not going to help. If it is material that hasn't been distributed, it is not going to help.

The Inspector General's report demonstrates the need for enactment of S. 1974, the Leahy-Grassley FBI Reform Act, to charter the authority of the FBI's Inspector General to review allegations of FBI misconduct and to strengthen FBI information management and technology and to protect FBI whistleblowers.

I will put the rest of my statement in the record. We will continue these oversight hearings, and I do want to extend my appreciation for the cooperation I have received from the FBI in going forward on this. It is a lot different than a few years ago, what the cooperation would be.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman LEAHY. Senator Hatch?

STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Senator HATCH. Well, thank you, Mr. Chairman. I apologize for being a little late. I had to introduce the Assistant Secretary of the Treasury.

Chairman LEAHY. Wearing that tie?

Senator HATCH. Yes, wearing my modest tie here.

Chairman LEAHY. This is how you tell the liberals from the conservatives on this committee. You will notice my dark tie.

Senator HATCH. The conservatives are so boring.

Mr. Chairman, I would like to start off by stating unequivocally that I consider the FBI to be one of the finest, if not the finest, law enforcement agencies in the world. But those who justifiably we hold in great regard also bear a great responsibility.

Last spring, we were all disappointed to learn that in the process of turning over millions of pages of documents to the defendants who were responsible for blowing up the Murrah Federal Building in Oklahoma City, the FBI had inadvertently failed to produce some documents. This is a mistake that never should have happened in litigation.

Fortunately, with respect to Timothy McVeigh and Terry Nichols, there was no basis for arguing that any of the documents that were not produced would have altered in any way the outcome of their trials. Next time, we may not be so lucky. I am therefore committed to doing everything necessary to ensure that these types of mistakes do not ever happen again.

The Department of Justice Inspector General has now completed a thorough and comprehensive review to determine how these documents fell through the cracks and how such mistakes can be eliminated in the future. And before I go on, I would like to acknowledge Glenn Fine, the DOJ Inspector General, for the fine work performed by you, Mr. Fine, and your staff. This report is clear. It is thorough and well-organized, and it should serve as a model for future investigative reports.

There is much good news in the IG report. First, and most importantly, there is nothing in the report that does anything that calls into question the validity of the convictions or the sentences imposed on Timothy McVeigh or Terry Nichols. While I recognize that the guilt or innocence of these men was not the focus of the IG's report, I nevertheless take comfort from the fact that the IG

uncovered no information that would even suggest that these men were not the perpetrators of the horrible crimes for which they were justly convicted. We must not forget that these men were captured, brought to trial and convicted for blowing up a Federal building and murdering more than 160 men, women and children through the hard work and through the dedication of FBI agents and personnel.

Second, I am gratified to learn that the Inspector General determined that the FBI had not purposefully sought to withhold these documents from the defense. The Inspector General found that in the midst of producing more than a million pages of materials, some 1,033 documents were not turned over, and that the failure to produce these documents was simply the result of human error, not misconduct or misfeasance or malfeasance on the part of the FBI.

Finally, I have been pleased to learn that under the vigorous direction and leadership of Director Robert Mueller, the FBI has already begun implementing many of the IG's suggested reforms. I applaud the IG for your thorough report, and I urge the FBI to continue its commitment to overhauling and upgrading its records management systems.

Let me make a final point. When the FBI does its job well, we rarely hear about it. There is no way to tell how many terrorist plots against the United States have been averted simply because of the existence of the FBI's counter-terrorist capabilities.

When the FBI does make the news, it is overwhelmingly for a job well done. It may be the perpetrator of a rape who has been identified and incarcerated because the FBI laboratory has matched his DNA to evidence found at the crime scene. Or perhaps a malicious computer virus has been detected by the FBI and traced back to a cyber criminal operating in a foreign country.

It is this positive record of effectiveness and efficiency that makes it so newsworthy when the FBI fails to perform its duty with the degree of care and professionalism that we have come to expect. And as a result, many times we make a lot more fuss about these matters than the matters that very few people know very much about that are successes.

As a United States Senator, I consider it to be one of my most solemn responsibilities to ensure that the awesome powers our law enforcement agencies have are exercised in a responsible fashion; that is, in a way that inspires confidence in our citizens and does not unlawfully infringe on our cherished liberties. I know that my colleagues on both sides of the aisle also feel the weight of this responsibility.

Oversight hearings such as the one we are holding today are important and I look forward to the testimony of the witnesses today. But based on my review of the IG's report, the written testimony submitted by the witnesses, and my own knowledge of what Director Mueller has accomplished during his short tenure as director, I am persuaded that the FBI is taking the appropriate steps to address the shortcomings in records management that were revealed by the Oklahoma City bombing case, and thereby maintain its position as one of the world's most effective law enforcement agencies.

So, Mr. Chairman, I appreciate your holding these hearings and I want to thank you for your efforts here today.

Chairman LEAHY. Thank you.

Our first witness will be Glenn Fine, who is the Inspector General of the Department of Justice. He is a graduate of Harvard Law School, a Rhodes Scholar, and a former Federal prosecutor. He served as the director of the Special Investigations and Review Unit, and now has served under two Attorneys General. I know on this one, he has done extremely thorough and detailed work.

I know that you put your own Director of Special Investigations, Suzanne Drouet, in charge of the Oklahoma documents matters, and I think that shows the importance you gave to it. We will put the whole report in the record, but I do want to hear from you, Mr. Fine, and then we will go to each of the other witnesses.

STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. FINE. Thank you. Mr. Chairman, Senator Hatch, members of the Committee on the Judiciary, I appreciate the opportunity to appear before the committee this morning to discuss the Office of the Inspector General's report on the belated production of documents in the Oklahoma City bombing case.

The disclosure of these documents just 1 week before the scheduled execution of Timothy McVeigh raised serious questions as to whether the FBI had intentionally failed to disclose documents to the defense before trial, and why the failure to produce documents had occurred. Because of the importance of these issues, the OIG expended significant resources to investigate the circumstances surrounding the belated disclosures.

The OIG team of attorneys, special agents and auditors was led by an OIG attorney whom Chairman Leahy just described, who is a former Federal prosecutor. The team conducted approximately 200 interviews of FBI and Department employees. On Tuesday of this week, we issued a 192-page report detailing our findings.

In sum, our investigation found that widespread failures by the FBI led to the belated disclosure of more than 1,000 documents in the OKBOMB case. We traced the failures to a variety of causes, including individual mistakes by FBI employees, the FBI's cumbersome and complex document handling procedures, agents' failure to follow FBI policies and procedures, inconsistent interpretation of policies and directives, agents' lack of understanding of the unusual discovery agreement in the case, and the tremendous volume of material being processed within a short period of time.

The failures were not confined to either the FBI field offices or the OKBOMB task force. Both share responsibility. However, we did not find that any FBI employees intentionally withheld from the defense documents they knew to be discoverable.

Our report criticizes most severely several senior FBI managers for how they responded when they became aware of the belated documents problem. The issue was first discovered in January 2001 as part of a routine archiving process by two conscientious analysts in the FBI's Oklahoma City field office.

These two analysts found copies of documents that had not been turned over to defense attorneys and materials sent by the offices

to Oklahoma City. Yet, the senior managers to whom they reported the problem failed to adequately manage the document review process and failed to set any deadlines for completing the project.

Most troubling, the managers failed to notify FBI headquarters or the prosecutors in the case until the beginning of May, 1 week before McVeigh's scheduled execution. We believe their failure to take timely action to resolve or report the problem was a significant neglect of their duties and we recommend that the FBI consider discipline for these failures.

Let me now turn to the question of why the documents were not produced before trial. We were able to determine a number of factors that contributed to the belated disclosures.

First, the FBI's system for handling documents is inordinately complex. Documents are stored in many different locations. Various data bases are used to track the documents, and information is placed on different types of forms that are handled in different ways.

Second, despite instructions to send everything to the task force, some agents failed to send documents because they deemed the information as insignificant to the OKBOMB investigation.

Third, some employees incorrectly assumed that other employees had sent the documents in.

Fourth, it appeared that many field offices did not follow instructions from the OKBOMB task force to search their files and ensure that all investigative activity had been properly documented and sent to the task force.

We found that the task force also shares responsibility for documents not being disclosed. For example, we found that documents sent to the task force were lost or placed in the wrong file drawer.

We carefully examined the allegation that the Government intentionally withheld documents it knew to be discoverable from the defense. We questioned FBI employees and former employees, analyzed circumstantial evidence, and investigated documents the defense alleged showed that the Government intentionally withheld exculpatory evidence. We concluded that the evidence did not support a finding that Government personnel withheld evidence it knew to be discoverable.

We also examined the actions of the FBI after the belated documents were publicly disclosed in May 2001. FBI officials at headquarters incorrectly placed blame on the FBI's computer system and FBI field offices, when the fault lay both with the field offices and the task force. In addition, we saw many untimely and inaccurate responses from the field offices to the directives in 2001.

The issues encountered in this case shine light on several of the FBI's longstanding problems: antiquated and inefficient computer systems, inattention to information management, and inadequate quality control systems. The FBI has both a paper and an electronic information system in place, neither of which is reliable. Although the belated documents issue was presented as a discovery problem, the FBI's troubled systems are likely to continue to impede its ability to perform its mission.

In our report, we detail many recommendations to help address the problems we found. Following are highlights of some of the recommendations.

First, the FBI needs to foster an attitude throughout the entire agency that information management is a critical part of the FBI's mission. It is not the glamorous part of the mission, but it is an essential part. Unless the FBI as an institution ensures that sufficient emphasis is placed on managing the mass of information it collects, problems will persist.

Second, FBI automation systems must be reliable and user-friendly and they must integrate data bases that are used for many different functions throughout the FBI.

Third, the FBI must simplify its document handling process. The FBI's current system requires paper documents to move through multiple steps and locations, creating many opportunities for them to go astray. The FBI also should reduce the mind-boggling variety of forms it uses.

Fourth, the FBI must provide increased training on its automation systems in document handling. They should be required core skills for FBI employees, including agents and supervisors, and refresher training also should be required.

In conclusion, the significance of this case is much broader than the impact of the problem in the OKBOMB investigation. The FBI has known about these problems for some time either because the OIG has discussed them in other reports or because the FBI has found them through its own reviews. But until recently, the FBI has made insufficient efforts to correct these deficiencies.

FBI employees need and deserve better computer systems and support. As the tragic attacks of September 11 revealed, the FBI will continue to be faced with cases of the scale and dimension of OKBOMB, and the lessons learned from it will continue to be important.

To adequately fulfill its responsibilities in major cases, as well as in smaller ones, the FBI must significantly improve its document handling and information technology. This requires a sustained commitment of resources and effort, but the FBI must make this commitment if it is to avoid the serious problems that occurred in the OKBOMB case.

That concludes my statement and I would be pleased to answer any questions.

[The prepared statement of Mr. Fine appears as a submission for the record.]

Chairman LEAHY. Thank you, Mr. Fine. One of the reasons why I and many others have been urging the administration to do what they can to speed up this ability to pull up information is because, as I said earlier, I worry when the FBI doesn't know what it knows. They have information that might stop a terrorist bombing or might stop something from happening, but if they don't know it is there, it doesn't help.

The rest of the panel will be Mr. Bob Chiaradio, who is the new Executive Assistant Director for Administration.

I believe you used to head the Tampa office. Is that correct?

Mr. CHIARADIO. Yes, sir.

Chairman LEAHY. Bob Dies is the Chief Technology Officer, a former IBM executive who was very helpful to the committee last summer. Bill Hooten is the new Assistant Director for Records

Management. He recently came to the FBI from a private sector position at SAIC.

A vote has started, and we will recess for about five or 6 minutes so that we can go over and vote because I don't want to interrupt the testimony of any of the three of you. I will come right back and we will begin the testimony of the remaining three and then go to questions.

I should note that Mr. Chiaradio will be the one who will testify, and Mr. Hooten and Mr. Dies will be there to answer questions, as they have for the committee before.

Thank you.

[The committee stood in recess from 10:01 a.m. to 10:19 a.m.]

Chairman LEAHY. Thank you for your patience.

Mr. Chiaradio, would you please go ahead?

STATEMENT OF ROBERT CHIARADIO, EXECUTIVE ASSISTANT DIRECTOR FOR ADMINISTRATION, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.; ACCOMPANIED BY BOB DIES, CHIEF TECHNOLOGY OFFICER, FEDERAL BUREAU OF INVESTIGATION, AND BILL HOOTEN, ASSISTANT DIRECTOR FOR RECORDS MANAGEMENT, FEDERAL BUREAU OF INVESTIGATION

Mr. CHIARADIO. Thank you. Good morning, Chairman Leahy, members of the committee. We appreciate the opportunity to be here to discuss the myriad of things we are doing in response to the issues properly identified by Inspector General Fine. We also appreciate this committee's longstanding interest in our ongoing efforts to rebuild our antiquated information infrastructure.

We commend Inspector General Fine and his staff for a thorough, objective, and independent examination of these issues. His report is instructive and his recommendations constructive. Because his findings go to the very heart of how we conduct one of our core functions, Director Mueller has had the report made available to all employees and has made it recommended reading for all FBI management and supervisory personnel. Its lessons will be part of our training and its relevance and importance will live far beyond today.

Last May, then-Director Freeh outlined for Congress the massive nature of the OKBOMB investigation and the virtual flood of documents and information created during this course. He also expressed regret that our shortcomings pertaining to the records had overshadowed the enormity of the sacrifices and accomplishments of those agents who successfully investigated this case.

He candidly admitted that, "We simply have too little management attention focused on what has become over time a monumental task. The seemingly mundane tasks of proper records creation, maintenance, dissemination and retrieval have not received the appropriate level of senior management attention. This episode demonstrated the mundane must be done as well as the spectacular." He then outlined a number of steps that the Bureau had embarked upon to fix some of these shortcomings.

On Tuesday, Director Mueller stated that "Sound records management and document accountability are at the heart of the FBI's ability to support investigations and prosecutions with information

integrity. There can be no doubt about the accuracy, completeness, and proper disclosure of the records we compile during our investigations and used by prosecutors in the support of prosecutions. The ability to maintain, access, and retrieve documents is critical to our mission and equally critical to protect the rights of those charged with crimes. It is also fundamental to robust information-sharing capacities, both functions which we are readily enhancing. In short, records management and integrity are core functions that demand the same level of attention and accountability as any function we undertake. It must be a part of the Bureau's culture."

As Inspector General Fine outlined for you, there are host of contributing factors. The methods we use to record and retrieve information are too complex. Our automated case system was not very effective in identifying information or supporting the investigation. Our technology was inadequate. We lacked a true information management system, and what we do have is not user-friendly. Many of our employees lack the training necessary to be fully engaged in an automated environment, and a host of other issues as well.

But what we thought when this issue first surfaced and what we believe now has been confirmed by Mr. Fine. This is not a computer glitch. Although a more robust system would have helped, it is a management and cultural issue which must be forthrightly confronted.

We can add technology, simplify our procedures, and dramatically reduce the opportunities for human error. Doing those things are relatively simple. What we must do and what we are doing is recognizing information management as the core function that it is. At all levels, we must lead the Bureau back to where the function is accepted as second nature. We must put in place the structures and automation that fully support this core function, and we must inculcate in every employee, ourselves included, that this new way of doing business is the only way acceptable. We must improve our records management practices, not simply automate what we have been doing for decades.

We are taking specific actions to address each concern raised by the Inspector General and a number of significant steps are well underway to overhaul our Bureau-wide records management capabilities to increase accountability for compliance with established record procedures and to put in place the training and skill sets necessary to bring about full acceptance of a near-paperless environment.

Borrowing a little from what my boss has said, with the help of the Congress we have restructured to recognize that the creation, maintenance, use and dissemination is a core function that must be fully supported by management as a priority.

We have created a Records Management Division to ensure executive direction and full-time oversight over all records policies and functions, consolidating all records operations to ensure consistency, thoroughness and accountability. A professional records management expert, Mr. William Hooten, here with us today, has been hired from the private sector to run that division. He has been charged with modernizing our enterprise-wide records systems, developing comprehensive, enforceable policies and procedures, and to ensure records integrity. He is also charged with putting in place

those quality control mechanisms that will detect anomalies and problems early on.

It is critical that we manage information, not just the systems that support our records. Congress has funded, and we are implementing, extensive agency-wide training aimed squarely at reforming our culture to one that exploits and incorporates technology in our everyday way of doing business.

Director Mueller is personally providing the leadership for this. We have retrained our employees on proper document production, management and retrieval, and the importance of records management as a core function. There will be continuous training over the course of an employee's career.

Of course, basic to any modern system of records is a modern information technology system, and modernization of our information technology, as this committee knows, is one of our top priorities. We are making sustained progress in this area. Congress has approved funding for the FBI to upgrade technology and infrastructure for organizing, accessing, analyzing and sharing information throughout the FBI and beyond.

We are replacing the now antiquated automated case system in favor of a multimedia, near-paperless virtual case file, with significant improvements and capabilities that greatly reduce the possibility that future documents will be misfiled, lost, or otherwise fail to be produced. The new system will dramatically decrease the potential for human error, both automatically doing many functions now done by manual intervention and by substantially reducing the number of opportunities for problems to occur that are inherent in our current systems.

This new case file document management system, designed with substantial input from street agents, will be of benefit in greatly simplifying the records creation and maintenance processes, being user-friendly, and allowing us to manage leads much more effectively.

The FBI's computer network is being completely revitalized to provide a data warehousing, collaborative environment, instead of application stovepipes. The creation of data warehouses and ample supporting networks provide easier and more robust access and sharing of information, and results in integrated data bases. The need for ad hoc crisis software applications will be eliminated. Private sector support which will allow commercial software and professional scanning, indexing and storage of documents is being used to move us rapidly out of the paper environment that was so vexing in the OKBOMB investigation.

All of these systemic changes and many others, including everything Mr. Fine recommended, are critical components to what must be a sustained agency-wide effort. These things are as important to protecting rights as how we execute warrants and testify in court. The challenge is great, especially the challenge of changing the culture. We believe we are on the way.

Finally, although his exhaustive investigation found no evidence of any intentional effort to withhold information from defense counsel, the Inspector General's report also criticizes actions of certain FBI personnel. We are reviewing these criticisms and will move

quickly to take any appropriate disciplinary action. In the end, there must be accountability.

At this time, I am prepared to present a brief demonstration on the prototype of the virtual case file that is currently in development or answer any questions, as the Chairman would like.

Chairman LEAHY. I assume throughout all that you are doing the appropriate firewalls, depending upon classification and that sort of thing.

Mr. CHIARADIO. Absolutely. Within the branch created by Director Mueller in my area of responsibility is a new Security Division. Integral to this new system will be overlays and internal security, external security and the like.

Chairman LEAHY. Go ahead with your demonstration.

Mr. CHIARADIO. Mr. Chairman and members, I have circulated before my testimony this morning four charts which I will refer to in the presentation as slides.

The first slide is basically a virtual case file. What we would have is a sign-in screen. The IG found that ACS was so difficult to use that many agents and supervisors had abandoned their effort to use it. In fact, they would rather rely on secretaries and administrative personnel.

Our current system is 1970's and 1980's technology, green screen emulators with F key functionality. For example, it takes more than a dozen screen entries just to enter one document and upload it into the system. The virtual case file is designed to operate in a browser-based technology, point and click, user-friendly, things that we are using today in our everyday lives. The presentation will be more intuitive.

Security will be essential, as the chairman asked, as an integral component. Access will be password-controlled, roll-based authorities, possessed of robust features for document management control, auditing unauthorized access, the things we found with the Hanssen investigation.

We will have system-wide activity approval logs which will track documents where they have been throughout the process from creation into the final system, through what approval processes they travel.

Chairman LEAHY. You will also be able to follow, then, who was picking these documents up, too?

Mr. CHIARADIO. Absolutely. The system will be able to show us who may have printed a document, who looked at a document, where the document is. When it is needed for discovery, it will be in one place. It can't be misfiled. It can only be printed or burned onto a CD and transmitted to the defense or to the prosecutors.

We have a case document access review, where the agents will be responsible to go in on their own on a certain that will be designed that they go in and they see who footprinted into their case, who was supposed to be in there and who not, with the responsibility to elevate those concerns when found.

I will take you to the second slide. Once we would sign into a case, a case agent would now see——

Chairman LEAHY. Incidentally, this kind of thing you are talking about—I am sure Judge Webster's review people are probably looking at, too, I would hope.

Mr. CHIARADIO. Ken Sensor, the Assistant Director in the Security Division, has had a series of meetings with Judge Webster and his committee.

Chairman LEAHY. Thank you.

Mr. CHIARADIO. On the second page, on the slide, we were getting to a case file management system. Typically, this would be the prototype of what an agent would see when they logged in in the morning. Although the paper obviously doesn't reflect it, there is a red arrow circling up in the top case. That is going to be indicative to a case agent or an investigative employee that something new has happened in their case. A lead has come in from another office, a serial has been sent to them, a supervisor has sent instructions. There is not a chance, again, for human error. We are trying to minimize at every opportunity where human intervention is necessary, to have automation and technology assist us.

What we would see here is the ability to track leads, to control documents, to know when there is a document and activity has taken place in the case. The virtual case file will be interactive, intuitive processes, the ability to see one's case and lead assignments on a screen, rather than in paper folders or in drawers or in file cabinets, intuitively, again, to point and click to a file in your area of interest.

We would, for example, in this case click onto the first case and bring you to slide three, and this would be what was going on in this particular case. Again, that arrow or that spinning red notification would show you that what had happened in that case was a photo spread had come in, which is something that we don't have in ACS. We don't have the ability to put in any scanning or multimedia. It is only documents that we may create in our own environment, nothing external from another agency, for example, no ability to put a picture in.

During the 9/11 attacks, shortly thereafter, I was the agent-in-charge in Tampa and headquarters wanted to send us pictures of the 19 hijackers. They couldn't use our infrastructure to do that. It had to be put on a CD-ROM and mailed to me.

Chairman LEAHY. Also, I would think that you could do that in a hurry. Another part that is helpful is so many times it is frustrating. You hear on the news, whether it is the FBI or the chief of police in a major city or somebody like that will say there has been this terrible crime. We have the description and artist's sketch of such-and-such a person, and whoever is reporting the news is talking about it and I think the average American sits there saying, well, put the sketch up so we can see it.

Also, in those cases where you have got something and the Bureau determines that it makes some sense to let the press know this, you can immediately disseminate it to hundreds of outlets, thousands of outlets, if need be.

Mr. CHIARADIO. Absolutely. The virtual case file is one part of Trilogy, and Trilogy is the big project that the Congress has funded for us. By this summer, we hope to have deployed to the field the robust network, the desktops, the hardware, and the presentation software. This notion of Trilogy is in a development stage now called joint application design with the contractors and the users.

An important point to add about the virtual case file with respect to multimedia capabilities is the chairman's comment is we don't know what we know. We don't know what we know because a lot of the information we obtain and we collect in our files remain in a paper format. They are externally generated. They sit in file cabinets.

The multimedia capabilities of the virtual case file will give us the ability to bring that information into a digital format into data warehouses, to be able to access it, to be able to work against it with robust search engines and the like.

The FBI's current document management system requires paper through multiple procedures and steps. The IG had found that and it was replete through his report. The quote was that it was "mind-boggling," the variety of forms. What we are doing in the virtual case file development is eliminating to a great extent the forms in our investigative cases. We are getting down to one form.

We are going to obviate the need to have multiple reporting and stovepiping of applications by designing on the front end what we may need as an organization and not have to create automation to compensate for forms that were designed in the 1930's, the 1940's and the 1950's. We need to not just automate, but we need to revitalize the way we do our business.

We would have this project, virtual case file, delivered, certified and accredited for some months. In the interim, under the direction of Mr. Dies, and also our Information Resources Division, we are going to do some things to ACS.

We are going to collapse those 15 screens to upload a form down to 2 or 3. We are going to get our work force trained and start to get them ingrained in a culture of using this new technology for our organization anyway—the point-and-click, the Web-basing. So by the time we turn on our virtual case file, we will be prepared.

We have a robust training program put in place not only on the hardware deployment but on the software deployment. We have about $20 million set aside to do enterprise-wide training to get our organization prepared.

The last thing I will show on slide four is just an example of the photo spread, things that we can't do today, have multimedia, simply just transfer a photo spread of Mohammed Atta, as I just gave you a graphic anecdotal example of what happened when I was running the Tampa field office.

ACS will allow full-text retrieval. It would be very time-consuming before we had this to even get anything out of ACS. You might not even know what you are looking for. The search engines that are available today to search my name—you would have to have all of the letters in almost exactly the right order to even know if I was in your system.

We are working with the intelligence community, with the Mormon Church on some of the search engines they use for genealogy review and research to put a more robust search engine in there so we can pick out information that may be in our data bases; foreign names, for example, as a good start.

The most important thing is to get our data bases together. With this virtual case file and the data warehousing that we are going to create, we are starting with the five most critical investigative

applications. We have about 42 that have been created as workarounds to a bad system.

Some of those investigative warehouses—the need for them will be obviated by what we are doing with these five new data base consolidations into one warehouse. The others are going to be addressed after Trilogy in future appropriations requests and in future efforts by our Information Resources Division.

I can answer any questions or I could go further. There are many features that we have in this prototype, but I wanted to just give you a few examples of how accurate Inspector General Fine's report was on our shortcomings and how we will use every possible thing we can as far as technology to minimize the opportunity for human error. But that is not the final answer. We need to do more. We need to do more culturally. We need to do things in our organization to put an emphasis on this, on the importance of data management.

[The prepared statement of Mr. Chiaradio appears as a submission for the record.]

Chairman LEAHY. You have so many superb men and women in the Bureau who are well-trained. They go through intensive training, as you know, and I want them to feel that when they are there what they are doing is actually being paid attention to, and if they are involved in cases, they are going to be heard.

Technology is not the only answer, of course, but if you have technology that really brings the Bureau together rather than balkanizing it, that is extremely important. But then you have to do what Mr. Fine's report points out. You have also got to go to the basic culture of the Bureau to make sure that as you break down the walls, you really want everybody in.

If I could, I would like to go back to the Inspector General. I want to make sure I understand the sequence of events correctly, and I was reading through the material last night.

In January, the potential discovery problem is first brought to the attention of the senior FBI official who was running an entire FBI field division. From that time until May 7, the FBI conducts a search in most every field office in the U.S. for documents which were not turned over. Memos were being sent. Documents were being shipped to Oklahoma City and analyzed there. Supervisors are flying in from Dallas to review the materials; they have meetings. So there is a wide-scale operation going on in the Bureau. As it is proceeding, documents are being discovered that people in the FBI suspect may not have been turned over to the defense, even though they should have been.

Now, I am assuming this is an ongoing process. All of these documents didn't simultaneously appear the morning of May 6. So am I right that it essentially happened over a 5-month period and no one in the FBI even mentioned this potential problem to either the prosecutors who were working with them on the McVeigh case or to officials in the Department of Justice?

Mr. FINE. That is correct. No prosecutor, no one in the Department of Justice knew about this issue until May 7.

Chairman LEAHY. What does that say about the atmosphere in the FBI and how you would deal with these kinds of problems?

Mr. FINE. I think that is not a good atmosphere. When we talked to the inspector in charge, Mr. Defenbaugh, and asked him why he didn't expose the potential problem, he had a number of reasons, including he wanted to research the problem, he wanted to ensure that he was thorough. But when we asked him why didn't you tell somebody in the Justice Department, a prosecutor, that you had a potential problem so that they could deal with it, one of the answers he gave was I didn't want it to leak out, I didn't want to cry wolf.

That, to me, discloses not a good relationship that you could not tell a prosecutor and let the prosecutor provide guidance on the appropriate way to deal with this potential issue, even if you think you may find documents later on. We believe that the Department of Justice and the prosecutor should have been notified, and should have been notified early.

Chairman LEAHY. Well, I would think so because I know then-Director Freeh, like Director Mueller today, both of them are people who want the rules followed. Whether they agreed or disagreed—I am not saying they did disagree, but whether they agreed or disagreed with the court's ruling on discovery, I don't think there is any question that former Director Freeh and current Director Mueller would want those rules carried out.

There is no question in my mind that Attorney General Ashcroft, just as his predecessor, Attorney General Reno—if there was an order for discovery, they would want it carried out. What worries me is that somebody down the chain puts the Attorney General and the FBI director and the court and ultimately the public in a difficult position.

Did any of the people you dealt with in the FBI accept responsibility for their actions or inactions, as the case may be?

Mr. FINE. We found actually a notable and distressing lack of accountability, particularly on this issue. When we were talking to the people involved, they would say that it was somebody else's job to notify the prosecutors; it was somebody else's job to ensure that the review of the documents was done in an expeditious way.

One person kept saying, well, I was just a consultant to the problem, or I was in the problem and I was out of the problem. We believe that many of them should have taken responsibility and ensured that the process was reviewed quickly; if there was a problem, in fact, and that the prosecutors in the Department of Justice and FBI headquarters be notified. And none of them took the appropriate actions, in our view.

Chairman LEAHY. The reason I ask these questions is not to beat up on the FBI by any means. In this case, the Timothy McVeigh case, all the accounts I have read of it—and I have talked with the prosecutors involved with it. Obviously, when I was prosecuting cases, I never had anything that horrendous. No prosecutor has ever had anything that horrendous prior to that time and we hope that they don't again.

I looked at that case as a textbook of the way a case should be run. You had a judge who knew what he was doing who was in control of the case. You had highly qualified defense attorneys, highly qualified prosecutors, and a case of enormous importance to the United States. It was handled well, and I am convinced of the

defendant's guilt. There is no question in my mind from everything that I have read about it that he was guilty; no question that the law was followed appropriately on the sentencing phase and death penalty phase. All of that was done very, very properly.

What I worry about is something like this, where there is a mistake and somebody saying I don't want to tell anybody, and it may end up jeopardizing that whole thing. You know as a former prosecutor in a case like that it would be the most difficult thing in the world to re-try that case. You could do it, but it would be twice as hard to re-try a case, usually, that it is to try it in the first place.

I worry about whether these kinds of mistakes in the handling of documents and information might be the same kinds of flaws that hampered the FBI's sharing of counter-terrorism information internally and with other agencies prior to September 11.

You state in your report on page 176, "The tragic attacks occurring on September 11, 2001, demonstrate that the FBI continues to be faced with cases of the scale and dimension of Oklahoma City, and the lessons learned from the Oklahoma City case continue to be relevant. Though Oklahoma City occurred over 6 years ago, the FBI's document management process remains generally unchanged, as does the technology on which it relies."

You further point out that the failure to manage information properly has important implications for the FBI's ability to share information, both with prosecutors and other law enforcement agencies, which you state is even more important in the wake of September 11. I happen to agree with you. I am very, very worried that these other agencies don't have it.

Do you think that these problems that you found hampered the ability of the FBI, our premier investigative arm in this country, from being able to adequately share counter-terrorism information prior to September 11?

Mr. FINE. I think the FBI is in the business of gathering, storing, tracking, analyzing and sharing information. If they don't have adequate technology and information systems to be able to do that, I think it does hamper them.

I can't say what happened in the September 11 cases, but the vulnerabilities that we found in the OKBOMB case, I believe, have significant impact and effect on its abilities throughout major cases, as well as in smaller cases. So I do believe that these issues affect everything the FBI does.

Chairman LEAHY. Thank you. Everybody agrees that given the current state of the FBI's information and computer technology, in one sense the FBI does not know all that it knows. Does anybody disagree with that?

[No response.]

Chairman LEAHY. Now, I talked to the Attorney General last November and I told him he was right to focus the Department of Justice and the FBI on protecting America from further terrorist attacks. I am glad to see that that focus was emphasized after September 11, but if you are going to plan effectively for the future, you have to know what worked or didn't work in the past.

I have asked the Attorney General to consider an internal review of the FBI's counter-terrorism performance prior to and bearing on the attacks of September 11 to see if there are any lessons that we

might learn there. I asked the FBI director last October to preserve all the FBI's records and information so that such a review could be conducted, even if we found areas where mistakes were made. It won't surprise you to know that Director Mueller said, of course.

Would that kind of review be useful?

Mr. FINE. I think reviews are useful to determine the lessons learned, the problems that occurred, and how to prevent it from happening in the future. I hope that this review is helpful in the information technology field. I believe other kinds of reviews can have important effects and help in the future. So I do believe that what we do, what the inspector generals do, performs a useful function.

Chairman LEAHY. Does anybody want to add to that?

[No response.]

Chairman LEAHY. I will turn to Senator Sessions.

STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. Thank you, Mr. Chairman. I really have the greatest respect for the FBI. I have worked with them for quite a number of years and seen the integrity and dedication of the agents, their intelligence and ability and training.

The judge said they are not disciplined. I think for the most part FBI agents are disciplined, but it is not a perfect situation. Mr. Fine, I think you are touching on the good and the bad there.

Director Mueller, I believe strongly, has the kind of experience to understand just this problem. He has been a big-time prosecutor of criminal cases all his life. He is a career prosecutor. He admires the FBI agents that he has worked with, and I have asked him about it. But I also believe he would understand how to avoid this kind of thing happening in the future. For that, I am very grateful that we have him at this time because it is time to confront some of the problems in the FBI and try to get past those.

Your report, Mr. Fine, seems to touch on that. Your answer to Senator Leahy's questions were, I think, candid and noteworthy and important.

Mr. Chairman, I love the FBI and I believe it is the premier law enforcement agency. You are correct. They are accountable to this Congress and to the American people, and this is the best way that the American people will have confidence in it, to have public hearings and talk about the problems. We should do that, and I salute you for going forward with this review.

There are good things, I think, here that maybe a lot of people didn't notice. It didn't surprise me at all. I think I understood precisely how this problem with the McVeigh case happened. It was not intentional, as you found. As a matter of fact, there would be no real motive in terms of hurting the defendant for an FBI office in Miami to fail to send in an insignificant document to the prosecutors in Oklahoma City, would there, Mr. Fine?

I mean, it was inadvertence and lack of attention to detail rather than some attempt to compromise the prosecution or hurt Mr. McVeigh's chances.

Mr. FINE. As I stated, we didn't find any intent on anybody's part to withhold discoverable documents that they knew to be discover-

able from the defense. It was a wide range of documents. Many of them were utterly useless and insignificant. There were documents in virtually every field office. It was a widespread failure that we found. We did not find it to be an intentional failure.

Senator SESSIONS. What happened was in that court, that judge looked at that prosecutor and issued an order about what would be disclosed. It was a broad disclosure order that required documents and any interviews relating to the case, I assume, to be disclosed.

Mr. FINE. Actually, Senator Sessions, it was an agreement by the Government and the defense for this broad discovery.

Senator SESSIONS. But essentially it was backed up by the order of the court. Is that correct?

Mr. FINE. I believe the court did recognize it and order it, but it was entered into by the Government. The reason they did that was to ensure that the defense got the evidence, to show that there would be fair access to the evidence, and also to try and avoid discovery disputes.

Senator SESSIONS. Well, you make a good point because I am not sure under the strict rules of evidence all these documents would have been admissible, Mr. Chairman. Mr. Fine makes a good point. In fact, they probably were not. What happened was the prosecutor voluntarily agreed to what we refer to as an open case file. We will give you all documents, all interviews related to the case.

What was the language they actually used?

Mr. FINE. The language was never written down. This was an agreement entered into by the prosecution and the defense and it was never memorialized in writing. But there was as clear understanding that all FBI 302s—that is, records of interviews, inserts, 1-A documents, evidence and other things—had to be turned over to the defense or made available to the defense.

Senator SESSIONS. So then a directive went out from the Oklahoma City investigative team to every FBI office in America, because this was such a big case and it impacted the Nation and leads were being run in every office in America, to send in all your information. Some of them did and some of them did not, and that is what caused the problem fundamentally?

Mr. FINE. Fundamentally, that is what happened. There were many directives sent to the field offices saying send in everything you have on the OKBOMB case, and we found that in many cases those offices didn't. And in many cases, they did send it in and it was lost at the task force.

Senator SESSIONS. Now, on the negative thing here to the FBI, I have sensed on occasion—and I will ask if you found it here—do you think some of the people who got those inquiries and those telexes to send in information said this is not discoverable stuff, we don't really have to turn this over, I am not sending it in? Do you think that possibly was in the back of some people's minds, even though the prosecutors and the judge and the defense counsel were expecting all documents to come in?

Mr. FINE. Yes, we found that. We found that some agents used what they thought was their discretion to say this is irrelevant, non-pertinent, and it doesn't need to be sent in. But we found that they should not have done that, that they were specifically directed

to send in everything and let the task force decide what had to be turned over. So, yes, that did happen.

Senator SESSIONS. Sometimes, people get to thinking instead of following the direction of their bosses, and that can be dangerous if you don't know all the facts in the case, as obviously here. So that really compromised the case, I would suspect, that kind of mentality, inadvertence or whatever.

All the documents—and how many were produced? Was it a million?

Mr. FINE. There were millions of documents made available to the defense. There were 27,000, I believe, memoranda of interviews. I think there were 13,000 pieces of evidence. There were millions of hotel receipts, motel receipts, rental car receipts that were being tracked and made available.

Senator SESSIONS. And many of them, as it turned out, had absolutely nothing to do with the case.

Mr. FINE. That is what the judge found.

Senator SESSIONS. I remember when I first began as a prosecutor we had a great prosecutor in the South District of Alabama. The FBI knew him and he was renowned. His name was Ruddy Favre. They have named one of the rooms in the Federal U.S. Attorney's office now for Ruddy. He died a number of years ago.

He would tell all young agents this: don't' you worry. If there is an error in this case, do not cover it up. Come and tell me as soon as possible and I will take care of you. He said that because he believed that there was almost a zero tolerance for any error in the FBI. The young agents were afraid that if they had made a mistake, if they told it, their careers could be ruined. They could be adversely disciplined for some decision in a complex matter that they hadn't had experience with and it would compound the error.

Do you think there is a culture afoot in the FBI that still makes agents reluctant or fearful about coming forward at the earliest possible date if they may have made an error, even an unintentional error?

Mr. FINE. Yes, I think it exists to come extent. I don't believe it is all over the FBI, but I think that attitude is present.

I remember testifying at a hearing before this committee last year at which Senator Danforth made that very point. He said the big problem is not the mistake, it is the failure to disclose the mistake. That is what he thought the FBI should focus on, ensuring that people who make mistakes feel free and come forward and disclose those problems. I agree with that.

Senator SESSIONS. To me, that is a problem we need to get beyond. You don't want to accept lack of highest possible standards. You don't want to accept mistakes on a regular basis, but you also want people to let you know. The official spokesman for the FBI in the official arena, the courts, is the United States Attorney.

Do you think that the agents could have been more forthcoming and could have been more cooperative with the prosecutors in the case on these subjects?

Mr. FINE. Well, I think in the case itself I don't have a comment on that. I believe that the FBI—and I want to point this out: This should not diminish the enormous efforts of the FBI in inves-

tigating OKBOMB and bringing to to a successful prosecution, including the person that we criticize, Mr. Defenbaugh.

He was the inspector in charge of that investigation and he deserves wide credit for the way he handled that investigation. We criticize strongly how he handled the problem when the belated disclosures came forward. He did not disclose that potential problem and we think he should have at an early stage. I don't think he intended to cover it up completely. I think eventually he was going to tell about it if all of the research confirmed there was a problem. We think, though, he should have disclosed that problem very early on.

Senator SESSIONS. Well, I think you are correct. I know Danny Defenbaugh and I know he is a good man. He gave his life to the FBI and his country, and I believe he was working with just incredible tirelessness to make this case successful. I am sure it is a great embarrassment and painful for him to have this event—after all the things that they did successfully in the case, have this event come back and cause a problem.

He did delay some reporting it. What was it, a month or 2 months?

Mr. FINE. No. From the end of January, when the problem was initially disclosed, it went to about March, when it was very, very clear that they had not been able to find the documents and that there was a significant number of problem documents. And he did not disclose it until May 7.

Senator SESSIONS. May 7, and that was shortly before the execution date?

Mr. FINE. The execution date was May 16.

Senator SESSIONS. So they decided to do their own internal review to make absolutely certain that this had to be disclosed. When they realized that it had to be, they did so, but late?

Mr. FINE. Well, the conscientious employees that I described, the two analysts, when they get the documents, they disclosed it to their supervisors, including Mr. Defenbaugh, and they went forward with their review. But even by March, it was clear that there was a problem with the documents and they continued their review until every single document had been analyzed and reviewed in this very time-consuming and laborious process.

That happened at the end of April, and so they were finally mailed to Mr. Defenbaugh on May 7 and he disclosed it then. But in our view, his failure to disclose the potential problem earlier was a significant neglect of his duties.

Senator SESSIONS. I would agree. I think there was a delay there, an unfortunate delay. It was not held too late in the sense of the case. He did do it before the execution date, but there was very little time. It should have been done sooner.

Thank you, Mr. Chairman. I have gone over my time.

Chairman LEAHY. I gave you extra time. It is an important point. We all recall that because they had been so late in reporting this, the Attorney General had to delay what had been the scheduled execution date in that case to have it reviewed. I said at the time I thought the Attorney General did the right thing. I also know in my private conversations with him he was not happy to have been put in that position. He had no problem in doing what was the

right thing to do, but he was not very happy that when they started knowing about this early in the year that nobody had come forward.

Senator Grassley has been at several other meetings, and this is an area where he has not only enormous expertise but has been heavily involved. I appreciate him stepping out of his other hearing and I would yield to him.

STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Well, I thank you, Mr. Chairman, for doing that, and I want to thank you on this issue and a lot of other issues for your cooperation with me, and particularly your leadership on the bill that we recently announced.

First of all, I want to take the time to commend General Fine. I don't know you very well, but I want to get well acquainted with you. I think this report and the work that you have done on the FBI investigation, the McVeigh documents, et cetera, have been worked the way that inspector generals ought to work.

I say that not only from my observation, but I have a former employee who has been observing inspector generals' work for a long period of time. He is no longer in my office, but he made a very positive comment to me about your work, and I kind of use that as a standard of judging some of the work. So I think I not only want to commend you for this report, but I think for doing what inspector generals should do.

The most important, key point there is independence, and if sometimes you don't feel you have the independence that I think inspector generals ought to have and I think that the law allows you, I hope you will let me know.

I think you have proven through this work to be genuine watchdogs. I think you have hit home the need for the FBI reform bill that was introduced by the chairman and me, and this would codify, as you know, the Inspector General's authority to investigate the FBI.

I would turn to Mr. Chiaradio and the rest of you, and bear with me if I am asking something that you have answered before, because I would like to hear it from you again. So maybe we need to followup with some dialog.

First, it was unclear to me, in the comments of the FBI and the Department of Justice officials this week, whether the FBI has really taken responsibility for the main cause of McVeigh document problems, and that is obviously and quite simply human error. The problem was more than just a terrible filing system and old computers.

I don't want to rehash the whole report, but it pointed out problems and mistakes at the top level at headquarters all the way down to field agents. So I want to make sure that, first, you agree with the IG that human errors up and down the FBI chain were the main cause of this problem.

Mr. CHIARADIO. Senator, absolutely. Through my remarks and through some of the conversations we have had here today, it is clear that we have a cultural change as much as we have anything. Technology and technology upgrades will absolutely assist us in

minimizing the opportunity for human error, but as an organization we need to change. We need to get to the sense of urgency and the attention to detail, as Director Freeh said, in the mundane as much as the spectacular.

I can tell you from the 6-months that I have served directly under the leadership of Director Mueller that he not only believes that, but I believe he believes it. He has had two separate meetings now with all of our special agents-in-change where I have heard his comments to that audience, where he expects accountability, he expects people to admit their mistakes, come forward quickly with them and move on and correct them.

He is inculcating that into the organization to every person in the organization, and I believe that he is making that difference. It is a leadership issue, Senator. It starts with the director and it comes through all of us, and I believe we are on our way to that.

Senator GRASSLEY. My second question deals with the National Infrastructure Protection Center. I am going to refer to it, as I think everybody does, as NIPC. I ask you particularly because of your being an expert on technology, so I would like to ask you about the director's plan for the FBI to swallow up NIPC by putting it in the Criminal Division.

I hope that you know that NIPC is supposed to share information with the private sector and issue warnings about threats. The private sector has some concern about NIPC, and particularly concern about that move. So why does the FBI want to turn an information analysis and warning center into a support office for criminal investigation?

Mr. CHIARADIO. Senator, I talked to the director about this issue this morning at our seven o'clock staff meeting in anticipation of your question. The director has made no decision with respect to the NIPC. He has authorized me at this point and at other times to let you know that he values your opinion. Clearly, he will not make any final decision without coming to see you.

Senator GRASSLEY. Thank you. I think I have made clear that I think it is a mistake. I will be glad to listen to that, but I hope you come around to the point of view that I have.

I understand that you are training new and current agents in computer and recordkeeping with what is referred to as back to basics and other things, but I would like to know how these new policies will be enforced. What I really would like to have you answer is, first, specifically what kinds of accountability measures there are for the FBI as a whole and individuals in the FBI. And, second, how are you going to make sure that the FBI doesn't have the same human error mistakes that led to the problems with the McVeigh documents?

Mr. CHIARADIO. To answer the first question about what mechanisms are in place, we have cumbersome manuals of operation, administrative and investigative. I believe that was part of the Inspector General's findings that we have too complex a recordkeeping system.

What we are planning on doing and what the director has recognized and has organized, too, is a separate records management division, consolidating our functions, our policies and practices, where they have been sprinkled through the organization, bringing

in an expert from the outside, and Mr. Hooten is here with us today, charging him with putting together a consolidated and more enforceable procedure on how we maintain, process, and otherwise retrieve and handle our information management; also, with the technology that we are hoping to develop and we are developing through Trilogy, minimize at every possible turn the point of human error or the intervention of human beings into a process and get technology to where that can be done.

We cannot completely eliminate the possibility for human error. We can't run as an organization of just computers. We are an organization of 28,000 strong, but to every extent we can possibly minimize the opportunity for error through technology, we will.

As far as our training, part of that development will be on-time and just-in-time training with our new systems. We have set aside upwards of $20 million between our hardware implementation and rollout and our software implementation and rollout just for the training of the work force to make sure that they know what they are supposed to do and how they are supposed to get it done.

The remedies for failing to do that are administrative, and they are also performance-related; someone doesn't get a good report card on their performance. What we are trying to do, as we are reviewing now the findings of the Inspector General, is looking at the more serious allegations when it has to do with the issues that were raised in that report objectively by our Office of Professional Responsibility and take appropriate action. The director is prepared to look objectively at what the Inspector General has found, look at the details behind his work and take appropriate action on personnel where necessary.

Senator GRASSLEY. My last point would be more of a statement than a question. I hope that I can ask you to convey to Director Mueller when you see him that I would expect to see him take some action against the worst individuals who made the worst mistakes in this McVeigh paper case which the Inspector General has investigated so thoroughly.

I am going to assume the best and believe that he will take such action because he promised so quickly in January to force FBI officials to repay the Government for attending the retirement party of one of the retirees on the taxpayer's dime. So I hope to see some swift action in this case as well. Everyone at the FBI certainly needs to know that personal accountability carries consequences.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much. Again, I thank you for the amount of time you have spent on this, not just now but over the years, in fact, and I appreciate that.

Especially now that we are down to the last few days of a session, if you look at the list of committees meeting, every one of us is sitting in about four different committees, and I appreciate the senior Senator from Iowa taking the time to come over here for this.

We will keep the record open for questions from others. I will put some of my own questions in the record and I think we can finish up on just a couple I have.

Mr. Hooten, in the IG report, as I read it, one of the recommendations is that the general counsel review the FBI's policy

regarding the destruction of documents while a case is pending. I have to imagine that you have warehouses full of documents, so you have got the management and other questions.

But in the Corporate and Criminal Fraud Accountability Act, which I introduced to respond to the Enron-Arthur Andersen debacle—and I am not in any way tying that connection, but what made me start thinking about these document things is the Majority Leader and Senators Durbin, Harkin and myself are trying to close the loopholes on the destruction of documents by people in the financial services business, for the obvious reasons in this particular case, but for others. It makes me think that we want to make darn sure that we, the Government, are way above any question of reproach in the same area about document retention.

Does the FBI have a clear policy on the destruction of documents while a case is pending?

Mr. HOOTEN. Senator, I think I have been there nine or 10 weeks now, so I am learning to.

Chairman LEAHY. Aren't you glad to be here?

Mr. HOOTEN. I am, sir. I am very honored to be here, quite frankly.

There are a couple of parts to the answer to this question. The first one is we do indeed have a lot of things that we need to destroy that are trash, quite frankly, extra copies of things, things that relate to things that have been destroyed 50 years ago. We just don't know what we have. I think you said that correctly. So that is one thing. We do need to get rid of that because that helps us be more efficient all the way through.

But the other thing is, with the new systems we will employ, we will know what we have and we will know when we have extra copies. We will know the retention period of certain kinds of documents. We have over 300 different classifications of records. Each one has a different kind of retention period, and so some we keep for 10 years, some we keep for 30 years, and so on. Some we accession to the National Archives at the end of a certain period, some we keep forever, others we can destroy at a certain time.

I am finding a variety of ways to manage that now. One of my roles is to try and get that down into a very simple, very manageable way by using technology. It is the only way we can do it. It is just too big a job to be able to really monitor, be able to destroy the things we legally must destroy at the times we need to, be able to keep those things we need to keep, and be able to know what we have got and what we don't have.

Chairman LEAHY. But do you agree with me that especially on pending cases that such a uniform policy is vitally important?

Mr. HOOTEN. Absolutely, sir.

Chairman LEAHY. I would feel that we must have something that both prosecutors and defense attorneys can say here is the rule; we know what is there and what it will be and we can go forward.

Mr. Dies, if I could ask you—having Senator Grassley here makes me think about this. We have worked together to craft S. 1974, the FBI Reform Act. We want the FBI director, whoever is the FBI director, to have the most effective law enforcement and counter-intelligence agency he can.

Long after I am gone or you are gone, or anybody else, or currently here in the Senate or in the administration or anything else, we are still going to face terrorism threats. We are still going to have people that are going to break the law, and I think that we want to make sure in the 21st century that we are able to respond as well as we can to keep the highest standards of our own constitutional history, and so forth.

Do you have a feeling or a position on S. 1974, the Leahy-Grassley Act?

Mr. DIES. I believe it is under review by the Department of Justice. A large part of it isn't in my field of expertise. The part of it that is that relates to information management—frankly, I thought you had both creative and constructive ideas in there, and I would hope you are successful in getting these enacted.

Chairman LEAHY. Does anybody else want to add anything? Mr. Fine?

Mr. FINE. I would like to add that the provision of your and Senator Grassley's bill that codifies the jurisdiction of the Office of the Inspector General over the FBI and the DEA is an important provision and we support that. We believe that it should be in the law so that people know it will continue and that another Attorney General, whatever he or she decides, knows that it is the law that the Inspector General has full authority throughout the Department of Justice. We support that.

Mr. CHIARADIO. Senator, in the other areas, again, the Department has not passed a comment on that.

Chairman LEAHY. I understand.

Mr. CHIARADIO. But we clearly have some things we are interested in in there that are very constructive, especially the SES disciplinary process, some things with our police force, and we are looking forward to seeing how the final Act comes out.

Chairman LEAHY. Well, we will continue to work with you. Everybody has respect for the FBI and our Department of Justice. We just want it to work because the threats are lot different than when the FBI started or anything else. We are not dealing with bank robber who hops in a 1930 Ford and goes running down a back road and you hope that maybe you can get the word to the sheriff in the next county to block him.

We are dealing with money, information and everything else being transmitted instantaneously around the world. Our threat is not so much today that we are going to have some army march against us or an air force fly against us. We are far too powerful for that. It is not going to happen.

I worry a lot more about a dozen well-committed people, who could care less what the penalties because they attempt to die in the attempt anyway, who drive a dirty bomb down Pennsylvania Avenue or across the Triborough Bridge or into Century City, in Los Angeles, or anywhere else. That worries me a lot more, and we want to be able to catch them. And as we have found tragically enough in the last few years, terrorists can be home-grown or they can be from abroad.

And during that time, we will still have all the fraud cases and the major criminal cases, and we just want to make it work. We have certainly shown no hesitation to give money from the Con-

gress, and we feel no hesitation to give you new powers. But with that money and those new powers comes the requirement for us not only to do our oversight, but for you to use it the best way you can. The four of you have a great deal of respect on both sides of the aisle here from the members, and utilize that and keep us posted.

I appreciate very much your being here, and we stand adjourned.

[Whereupon, at 11:20 a.m., the committee was adjourned.]

[Submissions for the record follow.]

[Additional material is being retained in the Committee files.]

SUBMISSIONS FOR THE RECORD

STATEMENT OF
FBI EXECUTIVE ASSISTANT DIRECTOR
ROBERT J. CHIARADIO
BEFORE THE SENATE COMMITTEE ON THE JUDICIARY
MARCH 21, 2002

Good morning Chairman Leahy. We appreciate the opportunity to be here to discuss the myriad of things we are doing in response to the issues properly identified by Inspector General Fine. We also appreciate this Committee's longstanding interest in our ongoing efforts to rebuild our antiquated information infrastructure.

We commend the Inspector General and his staff for a thorough, objective and independent examination of these issues. His report is instructive and his recommendations constructive. Because his findings go to the very heart of how we conduct one of our core functions, Director Mueller has had the report made available to all employees and has made it recommended reading for all FBI management and supervisory personnel. Its lessons will be part of our training and its relevance and importance will live far beyond today.

Last May, then Director Freeh outlined for Congress the massive nature of the OKBOMB investigation and the virtual flood of documents and information created during its course. He also expressed regret that our shortcomings pertaining to the records had overshadowed the enormity of the sacrifices and accomplishments of those Agents who successfully investigated this case. He candidly admitted that "we simply have too little management attention focused on what has become over time a monumental task ....the seemingly mundane tasks of proper records creation, maintenance, dissemination and retrieval have not received the appropriate level of senior management attention ... [and that] this episode demonstrated that the mundane must be done as well as the spectacular." He then outlined a number of steps that the Bureau had embarked upon to fix some of the shortcomings.

On Tuesday, Director Mueller stated that "Sound records management and document accountability are at the heart of the FBI's ability to support investigations and prosecutions with information integrity. There can be no doubt about the accuracy, completeness and proper disclosure of the records we compile during our investigations and used by prosecutors in support of prosecutions. The ability to maintain, access and retrieve documents is critical to our mission and equally critical to our

ability to protect the rights of those charged with crimes. It also is fundamental to robust analytical and information sharing capacities, both functions that we are rapidly enhancing. In short, records management and integrity are core functions that demand the same level attention and accountability as any function we undertake. It must be a part of the Bureau's culture."

As Inspector General Fine outlined for you, there are a host of contributing factors. The methods we use to record and retrieve information are too complex. Our Automated Case System (ACS) was not very effective in identifying information or supporting the investigation. Our technology was inadequate. We lacked a true information management system and what we do have is not user friendly. Many of our employees lacked the training necessary to be fully engaged in an automated environment and a host of other issues as well.

But what we thought when this issue first surfaced and what we believe now has been confirmed by Mr. Fine. This is not a "computer glitch," although a more robust system would have helped. It is a management and cultural issue which must be forthrightly confronted. We can add technology, simplify our procedures and dramatically reduce the opportunities for human error. Doing those things are relatively simple.

What we must do and what we are doing is recognizing information management as the core function that it is. At senior levels, we must lead the Bureau back to where this function is accepted as second nature. We must put in place the structures and automation that fully support this core function and we must inculcate in every employee, ourselves included, that this new way of doing business is the only way acceptable. We must improve our records management practices, not simply automate what we've been doing for decades.

We are taking specific actions to address each concern raised by the Inspector General, and a number of significant steps are well underway to overhaul our Bureau-wide records management capabilities, to increase accountability for compliance with established records procedures, and to put in place the training and skill sets necessary to bring about full employee acceptance of a near paperless environment.

Borrowing a little from what my boss has said, namely that with the help of Congress, we have restructured to recognize that the creation, maintenance, use and dissemination of our records is a core function that must be fully supported by management as a priority.

We have created a Records Management Division to ensure executive direction and full-time oversight over all records policy and functions, consolidating all records operations to ensure consistency, thoroughness and accountability.

A professional records management expert, Mr. William Hooton, here with us today, has been hired from the private sector to run the division. He has been charged with modernizing our enterprise-wide records systems and developing comprehensive, enforceable policies and procedures to ensure records integrity. He also is charged with putting in place those quality control mechanisms that will detect anomalies and problems early on. It is critical that we manage information, not just the systems that support our records.

Congress has funded, and we are implementing, extensive agency-wide training aimed squarely at reforming our culture to one that exploits and incorporates technology in our everyday way of doing business. Director Mueller is personally providing the leadership for this.

We have retrained our employees on proper document production, maintenance and retrieval and the importance of records management as a core function. There will be continuous training over the course of an employee's career.

And, of course, basic to any modern system of records is a modern information technology system, and modernization of our information technology, as this Committee knows, is one of our top priorities. We are making sustained progress in this area. Congress has approved funding for the FBI to upgrade technologies and infrastructure for organizing, accessing, analyzing and sharing information throughout the FBI and beyond.

We are replacing the now antiquated Automated Case System in favor of a multimedia and near paperless "virtual case file" with significant improvements in capabilities that greatly reduce the possibility that future documents will be misfiled, lost or otherwise failed to be produced. The new system will

dramatically decrease the potential for human error both by automatically doing many functions now done by manual intervention and by substantially reducing the number of opportunities for problems to occur that are inherent in our current systems.

This new case file document management system, designed with substantial input from street Agents, will be of benefit by greatly simplifying the records creation and maintenance processes, being user friendly, and by allowing us to manage "leads" far more effectively.

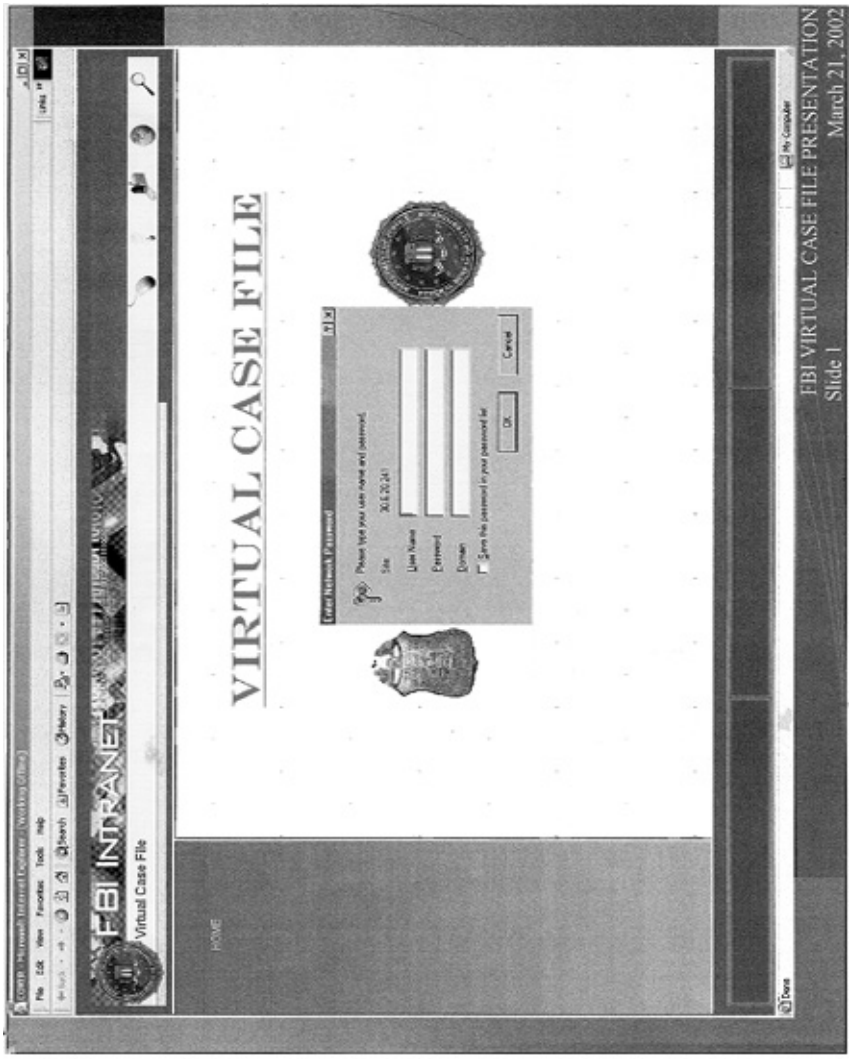
The FBI's computer network is being completely revitalized to provide a "data warehousing" collaborative environment instead of application "stove pipes." The creation of "data warehouses" and ample supporting networks provide easier and most robust access to and sharing of information and results in integrated databases. The need for ad hoc crisis software applications will be eliminated.

Private sector support will allow commercial software and professional scanning, indexing and storage of documents is being used to move us rapidly out of the paper environment that was so vexing in the OKBOMB situation.

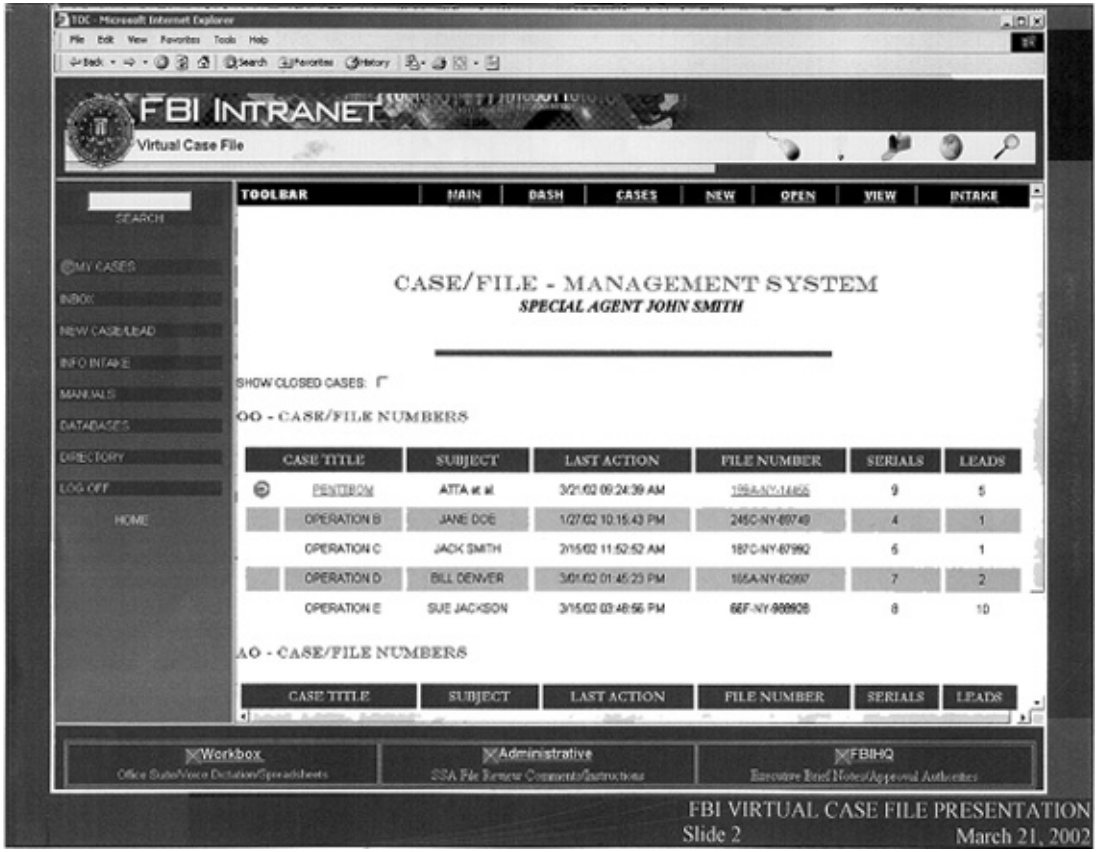
All of these systemic changes and many others, including everything Mr. Fine recommended, are critical components to what must be a sustained, agency-wide effort. These fundamental things are as important to protecting rights as how we execute warrants and testify in court. The challenge is great, especially the challenge of changing a culture. We believe we are on the way.

Finally, although his exhaustive investigation found no evidence of any intentional effort to withhold information from defense counsel, the Inspector General's report also criticizes the actions of certain FBI personnel. We are reviewing these criticisms and will quickly move to take any appropriate disciplinary action. In the end, there must be accountability.

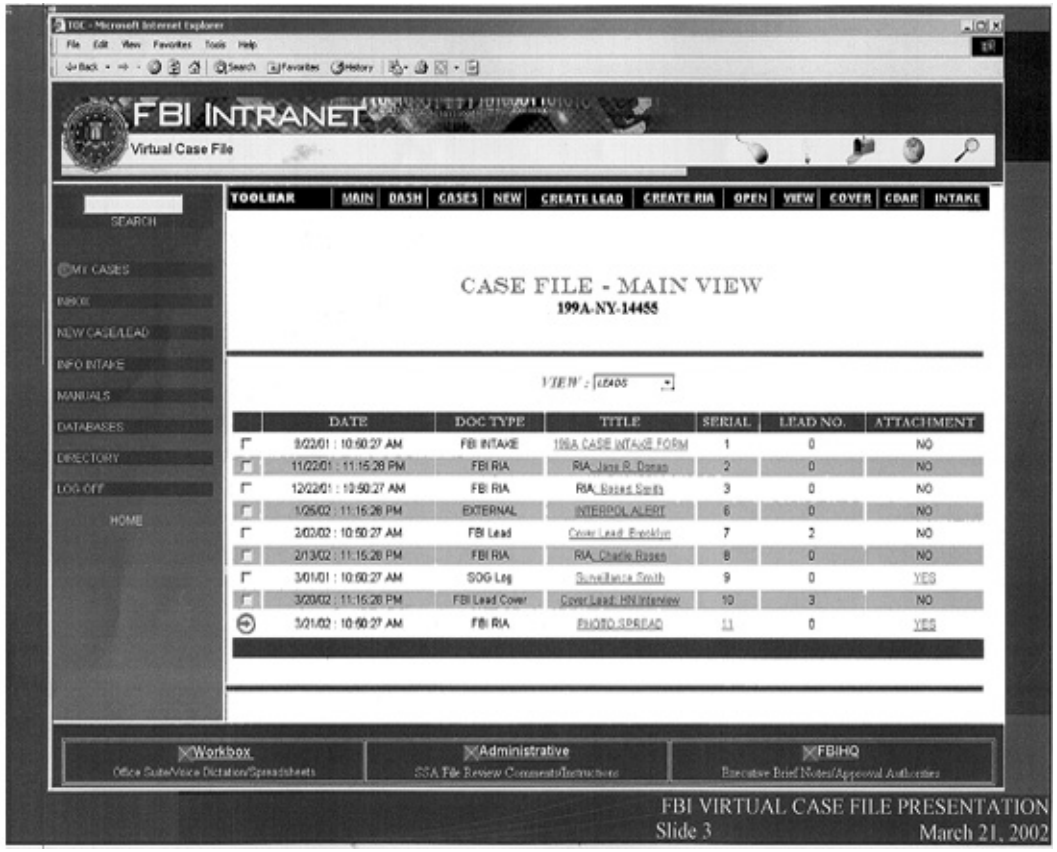
###



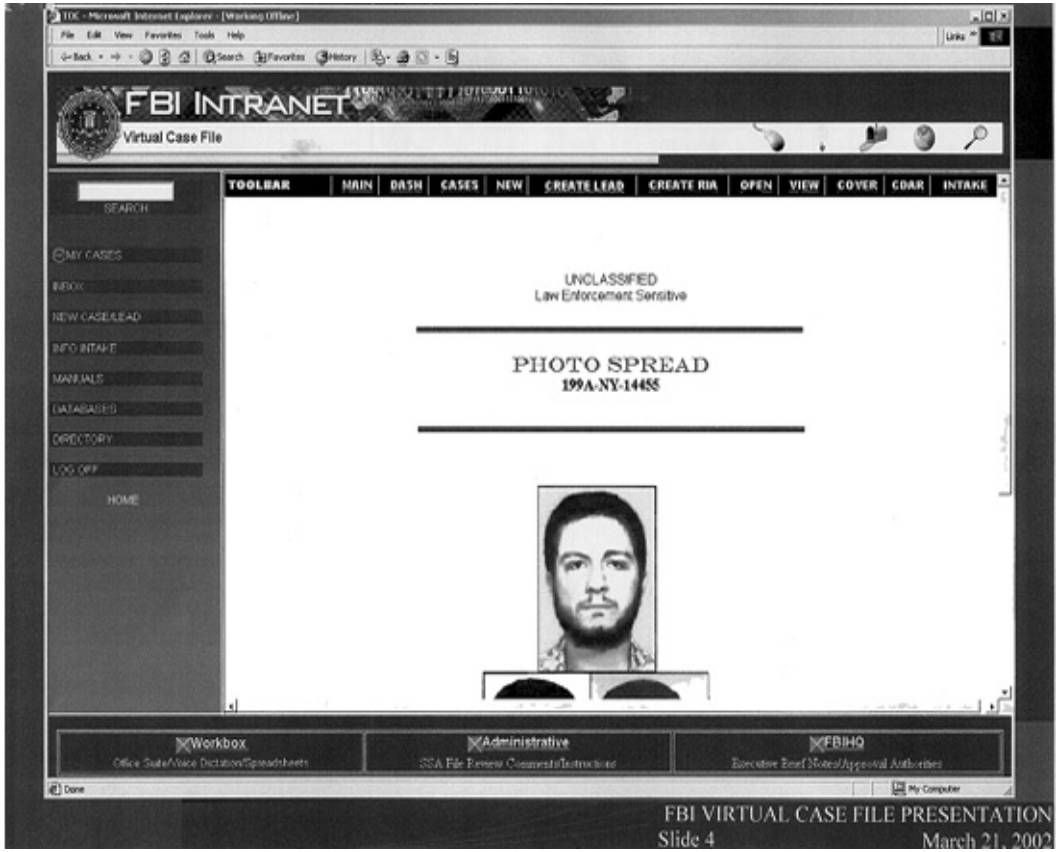
FBI VIRTUAL CASE FILE PRESENTATION
Slide 1
March 21, 2002



FBI VIRTUAL CASE FILE PRESENTATION
Slide 2 March 21, 2002



FBI VIRTUAL CASE FILE PRESENTATION
Slide 3
March 21, 2002



FBI VIRTUAL CASE FILE PRESENTATION
Slide 4
March 21, 2002

TESTIMONY OF .GLENN A. FINE
Inspector General, U.S. Department of Justice

Before the Senate Committee on the Judiciary
March 21, 2002

Mr. Chairman, Senator Hatch, and Members of the Committee on the Judiciary:

I appreciate the opportunity to appear before the Committee this morning to discuss the Office of the Inspector General's (OIG) report on the belated production of documents in the Oklahoma City bombing case. The disclosure of these documents just one week before the scheduled execution of Timothy McVeigh raised questions as to whether the Federal Bureau of Investigation (FBI) had intentionally failed to disclose documents to the defense before trial, and why the failure to produce documents occurred. Because of the importance of these issues, the OIG expended significant resources to investigate the circumstances surrounding the belated disclosures. We detail our findings in a 192-page report, which we issued on March 19. In my testimony today, I will summarize the findings of our investigation and discuss the systemic recommendations we made to help address the problems we found.

In sum, our investigation found that widespread failures by the FBI led to the belated disclosure of more than 1000 documents in the Oklahoma City Bombing case (OKBOMB). We traced the failures to a variety of causes, including individual mistakes by FBI employees, the FBI's cumbersome and complex document-handling procedures, agents' failures to follow FBI policies and directives, inconsistent interpretation of policies and procedures, agents' lack of understanding of the unusual discovery agreement in this case, and the tremendous volume of material being processed within a short period of time. The failures were widespread and not confined to either the FBI field offices or the OKBOMB Task Force; both share responsibility.

We did not find that any FBI employees intentionally withheld from the defense any documents they knew to be discoverable.

We are most critical of the way certain senior FBI managers responded when they became aware of the potential problem in January 2001. We found that they did not aggressively manage the document review process or set deadlines for the process to be completed. Most troubling, they waited until one week before the scheduled execution of McVeigh to notify FBI Headquarters or the prosecutors about the problem.

Our report also is critical of the way that FBI Headquarters handled the problem even after it was disclosed. We found that the instructions issued by FBI Headquarters to the field were confusing and contradictory. In addition, we found that many field offices failed to provide information and documents in a timely or accurate manner in response to requests in 2001.

This case highlights the significant weaknesses in the FBI's computer systems. They are antiquated, inefficient, and badly in need of improvement. Although we do not believe the failures in this case were caused by the computer systems, these systems cannot handle or retrieve documents in a useful, comprehensive, or efficient way, and they do not provide FBI employees with the type of support they need and deserve.

OIG Investigation

Before I provide more details about our investigation and findings, I want to first recognize the OIG employees who worked on this review. The OIG team consisted of five attorneys, two Special Agents, two auditors, a paralegal, and other support personnel. The director of the OIG office that conducts special investigations, a former federal prosecutor, led the team.

The team conducted approximately 200 interviews of current and former FBI and Department of Justice officials and visited 13 FBI field offices to conduct interviews, view the physical premises, and review office processes for handling documents. These 13 offices accounted for more than 50 percent of the more than 1,000 belated documents. The OIG also surveyed the 43 other FBI field offices for explanations about how they handled Oklahoma City bombing documents and why they failed to provide the materials to the Task Force.

In general, the OIG investigation sought to address the following questions:

1. How were the belated documents discovered in the FBI? Why were discoverable items not produced before the McVeigh and Nichols trials?

2. Did government employees intentionally conceal exculpatory information from the OKBOMB defendants?

3. Did the FBI act appropriately and timely upon learning that items sent by FBI field offices to Oklahoma City in 2001 might not have been disclosed properly to the defense before the Nichols and McVeigh trials?

I will address each of these issues in turn.

The Discovery of Belated Documents

Immediately following the bombing of the Murrah Federal Building, the FBI and the Department of Justice established a Task Force to investigate the crime. An FBI Inspector in Charge and a Department of Justice prosecutor led the Task Force, which at its peak consisted of over 200 investigators, prosecutors, and support personnel. The Task Force initially was located in Oklahoma City but later moved to Denver, Colorado, when the defendants' trials were moved. In addition to the personnel assigned to the Task Force, thousands of other investigators from the FBI's 56 field offices, its foreign offices, and other law enforcement agencies also participated in the OKBOMB investigation.

The belated documents at issue consisted primarily of FD-302s and inserts, forms used by the FBI to record investigative activity such as witness interviews. After FBI agents in the field offices memorialized their investigative activity on the appropriate form, the documents were supposed to be sent to the Task Force. Task Force personnel organized the evidentiary material, entered a brief description of the material into databases, and filed the hard copies into sub-files.

In every federal criminal trial, the defendants are entitled to have access to some, but not all, of the prosecution's files. After the OKBOMB defendants were indicted, however, the government decided to go beyond the discovery rules routinely used in federal criminal trials and agreed to provide the defense with all FBI FD-302s and inserts. The agreement was not formalized in writing, but we found no dispute about this obligation.

As the OKBOMB investigation progressed in 1995 and 1996, the Task Force realized that it was not receiving all of the documents generated in FBI field offices. On many occasions, the Task Force sent sternly worded instructions to the field offices that *all* OKBOMB-related materials were to be sent to the Task Force and directed the field offices to search their offices for OKBOMB materials. At the same time, however, some field offices complained to the Task Force that they were receiving multiple requests from the Task Force for documents that the field offices had sent previously.

In 1997, the OKBOMB defendants were tried in separate trials in Denver, after the trial judge moved the cases from Oklahoma City. Following the trials, the evidence was packed, transferred back to Oklahoma City, and stored in a large warehouse.

In early 2000, personnel in the FBI's Oklahoma City Field Office became concerned that the heating and cooling capacity of the warehouse was insufficient to maintain the OKBOMB evidence, and they sought the advice of the FBI's archivist. The archivist agreed that the warehouse was not suitable for long-term storage, and he also agreed to assist in the document preservation process.

In December 2000, the archivist sent an electronic communication to the FBI's 56 field offices authorizing them to destroy *copies* of OKBOMB documents that met specific guidelines the archivist provided. The field offices were to send a list of the remaining OKBOMB materials to the Oklahoma City Field Office.

In late January 2001, two field offices sent their OKBOMB files, rather than a list, to Oklahoma City. When two conscientious Oklahoma City Field Office analysts who had worked on OKBOMB examined the files, they immediately became concerned because they found what they believed to be original documents. Field offices should not have possessed any original OKBOMB documents, and they knew that the presence of originals in the field office could mean that the documents had not been sent to the Task Force or disclosed to the defense.

The analysts promptly disclosed the potential problem to William Teater, their supervisor in Oklahoma City, and to two senior FBI managers – Danny Defenbaugh, the Inspector in Charge of the OKBOMB investigation who became the Special Agent in Charge (SAC) of the FBI's Dallas, Texas, Field Office; and OKBOMB Supervisory Special Agent Mark White, who became a Supervisory Special Agent in the Dallas Field Office.

On January 30, 2001, the Oklahoma City analysts sent a communication to all FBI field offices instructing them not to destroy OKBOMB documents but rather to send all OKBOMB materials to Oklahoma City. As the material arrived, the analysts and a few additional Oklahoma City personnel compared every document against Task Force databases that listed the documents that

had been disclosed to the defense to determine whether these new documents had been disclosed previously.

In March 2001, the analysts showed Defenbaugh and White a box of problem documents that they had not been able to find in the databases that listed which documents had been disclosed to the defense. By the end of April 2001, the analysts had finished their examination of all the documents sent by the field offices and concluded that more than 700 documents had never been disclosed to the defense. Concerned about McVeigh's approaching execution date – originally scheduled for May 16, 2001 – the analysts mailed the documents to Dallas so Defenbaugh and White could determine how to handle the issue.

On May 7, 2001, Defenbaugh notified FBI Headquarters about the problem for the first time. The following day he notified Sean Connelly, an OKBOMB prosecutor, that documents that had not been turned over in discovery had been found in FBI files. This was the first that Connelly or any prosecutor was informed about the problem. On May 8, 2001, Connelly notified the defense about the discovery of the documents, and the next day he turned over 715 documents to the defendants' attorneys.

After this initial disclosure, the FBI continued searching for and finding additional documents in its field offices. These documents also were reviewed against the OKBOMB discovery databases, and by the end of May more than 300 additional documents were released to the defense. In total, 1,033 documents (consisting of more than 4000 pages) were provided to the defense.

Causes of the Belated Production of Documents

Because of the passage of time, the number of documents involved, and the inability of individuals to recollect exactly how they handled one document out of the many they created or gathered, it was impossible for us to ascertain with clarity the path of each belated document or why each such document failed to be turned over to the defense. Nonetheless, we were able to determine a number of factors that contributed to the belated disclosure of documents:

- The FBI's system for handling documents is inordinately complex. Many different employees are involved in processing documents, including agents, supervisors, and various administrative personnel. Documents are stored in many different locations, various databases are used to track the documents, and information is placed on different types of forms which are handled in various ways depending on the type of form.

- Procedural breakdowns added to the complexity of processing the OKBOMB documents. For example, in order to get information to the Task Force as quickly as possible, agents used teletypes (a form of instant communication similar, in some ways, to a facsimile) to send information. Yet, FBI and OKBOMB procedures required that information be placed in a different format – an FBI FD-302 or an insert. Some field offices believed information had been sent to the Task Force because they had sent a teletype but, because the Task Force did not have to disclose teletypes, the information was not ultimately provided to the defense.

- Despite instructions to send everything to the Task Force, some agents failed to send documents because they deemed the information as non-pertinent and insignificant to the OKBOMB investigation and therefore decided that the document did not need to be sent.

- Some employees assumed that other employees had sent the documents when none had. For example, agents in Resident Agencies (i.e., FBI satellite offices) created many of the belated documents. In some cases, Resident Agency personnel assumed that someone from their Headquarters' office had sent the document to the Task Force when in fact no one had.

- The Task Force repeatedly requested that the field offices send *all* OKBOMB materials to it. We concluded that it was likely that many field offices did not follow these instructions to search their files and to ensure that all leads had been properly documented and sent to the Task Force. In 2001 original documents were found in many of the same locations that the field offices had been directed to search.

We found that the Task Force also shares responsibility for documents not being disclosed to the defense. Documents that were sent to the Task Force were lost or placed in the wrong file drawer. For example, in our search we found some of the belated documents in the Task Force misfiled in subfiles that were not used to compile discovery. The problems in the Task Force's handling of documents were attributable to a variety of causes. The process used to move paper around the Task Force was cumbersome and the opportunities for documents to be misplaced were numerous. In addition, the Task Force did not have a routine policy of checking to ensure that items a field office said were being sent actually arrived at the Task Force.

The FBI did not have an effective automated quality control system to help the Task Force track documents when they were generated. Although the FBI assigns a serial number to every document it creates, in 1995 each field office assigned its own set of serial numbers to documents in its files, resulting in duplicate serial numbers. In order to generate a unique number for each document, the OKBOMB Task Force reserialized each document sent by the field office with an OKBOMB serial number. But Task Force supervisors did not recognize the deficiencies in their document processing system, and they gave little consideration to whether any measures should be taken to plug the gaps.

We carefully examined the allegation that the government intentionally withheld documents it knew to be discoverable from the defense. We questioned FBI employees and former employees, analyzed circumstantial evidence, and investigated evidence the defense alleged showed that the government intentionally withheld exculpatory evidence. We concluded, for the following reasons, that the evidence did not support a finding that government personnel withheld evidence it knew to be discoverable from the defense:

- We received no direct evidence that any FBI or Task Force employee intended to conceal exculpatory information.

- The evidence showed that, for the most part, the failure to provide documents and other items to the defense was caused by mistakes on the part of various individuals. In a few instances, we did find that agents had made the decision not to send certain items to the OKBOMB Task Force. The agents mistakenly believed that documents they judged to be non-pertinent to the OKBOMB investigation did not need to be sent to the Task Force. We do not believe these incidents show any intentional decision to withhold significant evidence from the defense.

- The belated documents did not contain a significant quantity or quality of previously unknown exculpatory information. We found that a significant portion of the belated documents concern useless information and would not have been discoverable in other criminal cases.

- The fact that the government disclosed information pretrial regarding allegations that persons other than McVeigh and Nichols had bombed the Murrah Building is evidence that the government was willing to disclose potentially exculpatory information.

As part of this inquiry, we also investigated eight belated documents that McVeigh's attorneys asserted were particularly significant and evidence of the government's intentional misconduct. We interviewed the agents who drafted the documents, their supervisors, and in some cases the administrative personnel who processed the documents. As a result of this review, we did not find evidence showing intentional misconduct. Rather, as with the other belated documents, the evidence indicated inadvertent breakdowns in the document handling process due to human error.

Analysis of the FBI's Actions in 2001

We also examined the actions of FBI officials after the belated documents issue arose in 2001. We considered whether FBI personnel acted appropriately upon learning that discoverable items may not have been timely disclosed to the defense.

When the two analysts in Oklahoma City discovered the potential problem with belated documents as part of the routine archiving process, they immediately notified FBI managers about the problem. We concluded that the managers who were informed of the problem – particularly Defenbaugh and White – did not adequately manage the review process of the OKBOMB documents. The analysts kept White and, through him, Defenbaugh informed that they were unable to find evidence establishing that many of the documents they were examining had been disclosed before the defendants' trials. Both White and Defenbaugh traveled to Oklahoma City in March 2001 and examined some of the documents that had been set aside as "problems." Yet, even then Defenbaugh and White did not determine how the files were going to be retrieved from the field or in what time frame. They did not set any timetable for completing the review and did not actively supervise the project or ensure that Oklahoma City managers were supervising it.

Most important, they did not notify the OKBOMB prosecutor, the FBI's General Counsel, or anyone else in FBI Headquarters about the potential problem. Their explanations for this failure varied, ranging from it was not their responsibility to do so, to not wanting to raise the problem until the review was completed, to being concerned about a possible premature leak about the problem. We do not believe their inaction was justified. We concluded that the failure by Defenbaugh and White to take timely action to resolve, or report, the problem of the belated documents was a significant

neglect of their duties, and we recommend that the FBI consider discipline for these failures.

We also criticize two other FBI managers, the supervisor of the two analysts and the SAC of the Oklahoma City Field Office, both of whom were informed about the review project, for not ensuring that the review process was completed expeditiously and the appropriate officials in FBI headquarters notified.

By contrast, we believe that the two analysts should be commended for their recognition and reporting of the problem.

FBI Actions After Learning About the Belated Documents

We also concluded that FBI officials at Headquarters failed to effectively address the document problems after they were notified in May 2001. Early statements about the cause of the problem incorrectly placed blame on the FBI's computer system and FBI field offices, when the fault lay with both the field offices and the Task Force. Communication with the field offices was deficient and led to some field office SACs learning of the problem from the media. In addition, Headquarters officials gave instructions to the field without a complete understanding of the nature of the problem. Their instructions were confusing, contradictory, and incomplete, which resulted in field offices having to complete multiple and duplicative time-consuming searches.

In addition, we saw many inadequate, untimely, and inaccurate responses from the field offices to the directives in 2001. Although these failures did not cause the belated documents problem, they raise serious questions regarding the FBI's attention to detail, managerial accountability, and the reliability of information sent by field offices to Headquarters and to other field offices.

For example, we found that some field offices reported in January 2001 that they had no OKBOMB documents only to later send boxes of documents to Oklahoma City in May 2001. In addition, some field offices appeared to have "lost" the FBI archivist's December 2000 request for OKBOMB documents and never took any action on it even though the request was sent electronically. In addition, although the January and March 2001 requests from Oklahoma City for OKBOMB documents were marked as requiring "immediate" action, in many instances the field offices took weeks or months to respond.

Destruction of Documents

As described earlier, through an electronic communication dated December 20, 2000, the FBI archivist authorized FBI field offices to destroy copies of OKBOMB documents that remained in their files if the field office followed guidelines set out in the communication. Our investigation found that 2 field offices had destroyed documents before the archival process had begun, and 13 field offices destroyed some portion of their OKBOMB files following the archivist's authorization. Of the 13 field offices, only one reported following the archivist's instructions.

We attempted to determine whether these field offices had destroyed any FD-302s or inserts – in other words, the type of documents that were covered by the discovery agreement. Nine field offices either acknowledged destroying such documents or could not rule out the possibility that they had been destroyed.

These nine offices insisted, however, that they destroyed only copies of materials that had been sent to the OKBOMB Task Force. While probably true with regard to most of the destroyed documents, it is impossible to verify that all the destroyed documents previously had been sent to the Task Force. Furthermore, even if the documents had been sent to the Task Force, the information might not have been disclosed to the defense. Without the actual documents to compare with the FBI databases, it is impossible to determine with certainty whether all the destroyed documents had been disclosed to the defense.

Recommendations

Although our investigation revealed numerous problems with the FBI's handling of the documents in this case, we also believe the failings need to be placed in context. The OKBOMB Task Force and the FBI field offices were dealing with what, at that time, was the largest criminal investigation ever undertaken by a United States law enforcement agency. The FBI processed millions of documents and items of physical evidence, conducted thousands of interviews, and managed an investigation that involved thousands of investigators and support personnel from the FBI and other agencies. The belated documents problem should not diminish their efforts.

Rather, the problems encountered in this case shine light on several of the FBI's long-standing problems: antiquated and inefficient computer systems; inattention to information management; and inadequate quality

control systems. And although the belated documents issue was presented as a discovery problem, the FBI's troubled information management systems are likely to have a continuing negative impact on its ability to properly investigate crimes. At the end of our report, we set forth recommendations to help address these systemic weaknesses.

Most of our recommendations relate to FBI computer systems and document management. The FBI initiated an automation system in 1995 that could address, in large part, the problem that we saw in OKBOMB – the inability of case investigators to know what documents have been created by other FBI investigators. The FBI's document management system – the Automated Case Support (ACS) system – utilizes "universal serialization" for document management. In any given case, all documents pertinent to a specific investigation are given serial numbers that follow sequentially regardless of the field office that created the document. Accordingly, case investigators can easily tell if they are missing the paper copy of a particular document because there will be a gap in the sequence.

We found, however, that ACS is so difficult to use that many agents and supervisors have abandoned the effort. As a result, the FBI has both a paper and an electronic information management system in place, neither of which is both reliable and effective.

The FBI is now in the process of developing upgraded information technology systems as part of a project it calls Trilogy. We did not investigate Trilogy as part of this review and therefore cannot state whether ultimately it will solve the FBI's substantial information management problems. But the success of any system depends on the FBI's full commitment to its use. All FBI employees must be fully trained on the system, and the efficient use of automation must become part of the basic job requirements for all employees, not only administrative support personnel but also agents and managers.

Following are some of the specific recommendations we make:

1. Commitment to Automation and Focus on Information Management

Most of the senior managers to whom we spoke acknowledged that they had no understanding of ACS, did not use it, and relied on their secretaries to obtain for them information off of the computer. They complained that the system was too difficult to use. Indeed, about the only consistent information we received during our investigation was the universal dislike for ACS by supervisors, agents, and support personnel. On the other hand, personnel in the FBI's Information Resources Division believed that some of the complaints

about ACS were the result of field managers' and FBI Headquarters' lack of commitment to automation – in other words, the system seemed cumbersome because employees refused to familiarize themselves with it.

In the past, the FBI has tolerated the development of duplicative systems: one paper and one automated. The FBI is simply too big and the cases are too large to continue to rely on paper as the chief information management tool. And because the FBI has tolerated the continued reliance on paper, the FBI's automation systems have suffered. Inefficiencies have been created, such as when field offices wait for the "electronic communication" to arrive through the mail before acting on it. In addition, when some employees are not utilizing the automated system properly, the data in the system becomes unreliable because it is not complete.

Any new automated system will meet the same fate as ACS unless FBI managers commit to using it and enforce its use throughout the FBI. We believe that the FBI must commit to relying on automation as the primary means for accessing, retaining, and transferring information.

The FBI also needs to foster and maintain an attitude throughout the agency that information management is an important part of the FBI's function, and commit to addressing deficiencies in a concerted manner. On several occasions the OIG has issued reports indicating that the FBI had significant problems in the way it handled documents and information, yet not enough was done to address the deficiencies raised.

For example, in a July 1999 report that the OIG issued on the Justice Department's Campaign Finance Task Force, we carefully tracked ten critical pieces of intelligence information and how they were handled by the FBI and the Department. We found that key information from the critical documents at issue either had not been entered into ACS in a manner that could be searched or had not been entered into ACS at all. We also found that many of the FBI personnel we interviewed were not well versed in the use of the FBI's database system and had erroneous beliefs about the way it operated. We recommended that the FBI amend its practices and regulations so that more information was entered into ACS and its computer databases. We also recommended supplementary training for FBI agents on ACS, which we called "crucial to the integrity and utility of the ACS system." Yet, despite agreeing to create a "working group with representatives from affected divisions/offices to revise procedures" and to develop a program to provide agents with additional training on ACS, the FBI did not implement these actions.

In another OIG report completed in February 2001, the Lost Trust report, we described significant failures by FBI agents who failed to turn over evidence

to prosecutors during a series of cases that began in 1989 into corruption in the South Carolina General Assembly. In those cases, the FBI failed to disclose to prosecutors important FD-302s and failed to disclose others in a timely fashion. We concluded that the documents were not intentionally withheld, but that the FBI's failure to produce these documents was the result of inadequate recordkeeping and inadequate organization of the files, which was exemplified by the fact that FBI agents and prosecutors had to depend upon the records of the defense counsel's paralegal to determine whether and when a document had been produced in discovery. We described how the FBI's case files were in substantial disarray and how the FD-302s were not even filed in the official file. We concluded that the FBI agent on the case was overwhelmed with the amount of work and that FBI managers provided insufficient support to ensure that the files were properly organized.

These reports illustrated significant deficiencies in the attention the FBI has given to handling documents appropriately or correcting deficiencies. The reports also show that even in cases involving many fewer documents, the FBI had difficulty tracking and processing its documents effectively.

Unless the FBI as an institution ensures that sufficient and long-term emphasis is placed on managing the information that it collects, problems will continue to exist. The problems may not be as publicly exposed as they were in OKBOMB, but they will continue to bedevil individual agents and prosecutors. We also would note that although the problem has been framed in this case in terms of the defense not obtaining access to certain material, some of the information also did not get to the prosecutors. The failure to manage information properly has important implications for the FBI's ability to share information, both with prosecutors and other law enforcement agencies. When information must flow through cases, agents, and even agencies, the FBI must have in place a reliable, trustworthy, and useful information management system. This is even more important because of the need for sharing information in the wake of September 11.

2. User Friendly and Reliable Document Management Systems

We found that relatively simple tasks in ACS require multiple steps and, frustratingly, the system "crashes" or "freezes" regularly. Many times when we interviewed administrative employees at FBI field offices and asked them to demonstrate ACS, the system stopped working.

While ACS allows full-text retrieval, it is very time-consuming and therefore not an effective case management tool. The FBI's case management

system must have the ability to conduct quick searches. In addition, the FBI needs to combine its various databases. For example, in the OKBOMB case the FBI used ACS to catalog documents, Rapid Start to track leads, and ZyIndex for full-text retrieval. Using separate systems to manage particular cases presents a series of problems, including the difficulty of training FBI personnel on how to effectively use the multiple systems. Further, increasing the number of database systems increases the chances that information will not be found, since not every FBI employee will think to check every system.

In one of several criticisms about the FBI's lack of current technology, FBI officials noted that employees of the FBI – an agency that needs to gather information – only had access to the Internet through a limited number of machines and could only e-mail other FBI employees.

As the FBI develops its next generation of information-management systems, we urge it to consult extensively with its agents, supervisors, and administrative personnel so that the people who actually use the system will have a say in how a system can be designed to meet their needs.

3. Simplification of Recordkeeping

The FBI's current document management system requires paper documents to move through multiple procedural steps and multiple physical locations. We recommend that the FBI work toward simplifying and automating its document management system. For example, FBI supervisors should be able to review electronic versions of documents rather than having paper sent from agents to secretaries to rotors and then to supervisors.

In addition, the FBI should reduce the mind-boggling variety of forms currently in use. For example, although we were told the difference between FD-302s and inserts, in practice they both appear to contain substantive information. In fact, in OKBOMB the inserts were disclosed to defense attorneys because prosecutors could make no useful distinction between the information on the inserts and the information on FD-302s.

The FBI has many procedures governing document and evidence processing, including such minutiae as prescribing when pencil or specific colored ink should be used for certain tasks. Despite these detailed procedures, we found considerable variation among the field offices. The FBI should simplify its forms and procedures, but ensure that they are being followed.

4. Training

The FBI's training on its automated systems is inadequate. We found that new agents received 10 hours of training on ACS. Two in-service classes are also offered: a 2-day class that most agents eventually take and a 3-day class usually taken by support personnel. We were told that 10 hours was insufficient to teach new agents how to effectively use ACS. During our review, the FBI Information Resources Training Unit, which is responsible for new agent and in-service computer training, also told us they believed that they had not received clear guidance as to what ACS skills agents need to perform their jobs effectively. Therefore, the training unit believed that it was not necessarily teaching the minimum set of skills agents needed.

In addition, new agents are not required to demonstrate minimum competence in ACS to graduate from the FBI's training academy. However, agents-in-training are required to demonstrate core skills in firearms, knowledge of legal issues, and investigative techniques. We believe the FBI should consider adding computer usage as one of the core skill requirements needed to graduate from the training academy.

The FBI should consider requiring mandatory refresher training on its automated systems and document handling for all employees, especially managers and supervisors. The FBI requires employees to regularly requalify on their firearms proficiency. We believe similar attention should be paid to training on automation and information management.

5. Post-Case Reviews

As part of our investigation, we interviewed prosecutors and senior investigators who participated in other major FBI cases, and we found no formal process in place for learning from these prior experiences. We recommend that the FBI and the Department of Justice initiate a post-case review process and develop case management protocols for large investigations like OKBOMB. Substantial time and effort can be saved if the case investigators and prosecutors do not have to reinvent administrative and substantive solutions to problems and issues that commonly arise during major cases.

Conclusion

The significance of the belated documents and the OIG investigation of the circumstances surrounding them is much broader than the impact of the problem on the OKBOMB case. We found a wide variety of flaws in the FBI's information systems and document handling that the FBI has known about for some time, either because the OIG has discussed them in other reports or because the FBI has found them through their own reviews.

However, until recently, the FBI has made insufficient efforts to correct the deficiencies. The FBI's information technology systems and procedures for handling documents was – and still is – inordinately cumbersome and badly in need of repair. The FBI's computer system cannot handle or retrieve documents in an efficient, useful, or comprehensive way. FBI employees need, and deserve, better computer systems and support.

As the tragic attacks of September 11 revealed, the FBI continues to be faced with cases of the scale and dimensions of OKBOMB, and the lessons learned from OKBOMB continue to be important. To adequately fulfill its responsibilities in major cases, as well as in smaller ones, the FBI must significantly improve its document handling and information technology. This requires a sustained commitment of resources and effort, but we believe the FBI must make this commitment if it is to avoid the serious problems that occurred in the OKBOMB case.

I would be pleased to answer any questions.

Statement of
The Honorable Orrin Hatch
United States Senator
Utah

March 21, 2002

PRINTABLE VERSION

Mr. Chairman, I would like to start off by stating, unequivocally, that I consider the FBI to be one of the finest - if not the finest - law enforcement agencies in the world.

But those who we justifiably hold in great regard also bear a great responsibility.

Last spring, we were all disappointed to learn that, in the process of turning over millions of pages of documents to the defendants who were responsible for blowing up the Murrah Federal Building in Oklahoma City, the FBI had inadvertently failed to produce some documents.

This is a mistake that never should have happened. Fortunately, with respect to Timothy McVeigh and Terry Nichols, there was no basis for arguing that any of the documents that were not produced would have altered, in any way, the outcome of their trials. Next time we may not be so lucky. I am therefore committed to doing everything necessary to ensure that these types of mistakes do not happen again.

The Department of Justice Inspector General has now completed a thorough and comprehensive review to determine how these documents fell through the cracks and how such mistakes can be eliminated in the future. And before I go on, I would like to acknowledge Glenn Fine, the DOJ Inspector General, for the fine work performed by him and by his staff. This report is clear, thorough, and well-organized, and it should serve as a model for future investigative reports.

There is much good news in the IG report. First, and most importantly, there is nothing in the report that does anything that calls into question the validity of the convictions or the sentences imposed on Timothy McNichols or Terry McVeigh. While I recognize that the guilt or innocence of these men was not the focus of the IG's report, I nevertheless take comfort from the fact that the IG uncovered no information that would even suggest that these men were not the perpetrators of the horrible crimes for which they were convicted. And we must not forget that these men were captured, brought to trial, and convicted for blowing up a federal building and murdering more than 160 men, women and children through the hard work and dedication of the FBI agents and personnel.

Second, I am gratified to learn that the Inspector General determined that the FBI had not purposefully sought to withhold these documents from the defense. The

Inspector General found that, in the midst of producing more than a million pages of materials, some 1,033 documents were not turned over, and that the failure to produce these documents was simply a result of human error - not misconduct or malfeasance on the part of the FBI.

Finally, I have been pleased to learn that, under the vigorous leadership of Director Robert Mueller, the FBI has already begun implementing many of the IG's suggested reforms. I applaud the IG for his thorough report and urge the FBI to continue its commitment to overhauling and upgrading its records management systems.

Let me make a final point. When the FBI does its job well, we rarely hear about it. There is no way to tell how many terrorist plots against the United States have been averted simply because of the existence of the FBI's counter-terrorist capabilities.

And when the FBI does make the news, it is, overwhelmingly, for a job well done. It may be the perpetrator of a rape, who has been identified and incarcerated because the FBI laboratory has matched his DNA to evidence found at the crime scene. Or perhaps, a malicious computer virus has been detected by the FBI and traced back to a cyber-criminal operating in a foreign country.

It is this positive record of effectiveness and efficiency that makes it so newsworthy when the FBI fails to perform its duty with the degree of care and professionalism that we have come to expect.

As a United States Senator, I consider it to be one of my most solemn responsibilities to ensure that the awesome powers our law enforcement agencies are exercised in a responsible fashion - that is, in a way that inspires confidence in our citizens, and does not unlawfully infringe on our cherished liberties. I know that my colleagues, on both sides of the aisle, also feel the weight of this responsibility.

Oversight hearings, such as the one we are holding today, are important. I look forward to the testimony of the witnesses today.

But based on my review of the IG's report, the written testimony submitted by the witnesses, and my own knowledge of what Director Mueller has accomplished during his short tenure as Director, I am persuaded that the FBI is taking the appropriate steps to address the shortcomings in records management that were revealed by the Oklahoma City bombing case, and thereby maintain its position as one of the world's most effective law enforcement agencies.

####

- TOP OF THIS PAGE
- RETURN TO HOME

PRINTER FRIENDLY VERSION

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

STATEMENT OF SENATOR PATRICK LEAHY,
CHAIRMAN, SENATE JUDICIARY COMMITTEE
FBI REFORM SERIES
HEARING ON
"REFORMING THE FBI IN THE 21ST CENTURY:
LESSONS FROM THE OKLAHOMA CITY BOMBING CASE"
MARCH 21, 2002

Today we resume our FBI oversight hearings that began last summer with a focus on the FBI's readiness to deal with the law enforcement challenges of today as well as tomorrow. These hearings are vital because, as we begin this new millennium, the FBI faces unprecedented challenges and also wields unprecedented power. With the stakes so high for the American people, it is the Committee's responsibility to ensure that the FBI is as great as it can be, and this series of bipartisan FBI oversight hearings is a fundamental part of the process.

The Inspector General's Findings

Specifically, today we consider the FBI's belated production -- and, as the important and thorough report by the Inspector General revealed this week – also the destruction of documents in the Oklahoma City bombing case. Even more troubling is the report's conclusion that senior FBI personnel failed to notify either the prosecutors on the case or high-ranking Justice Department officials, including the current FBI Director Robert Mueller, who was then serving as the acting deputy attorney general, about the belated document production problems until one week before the scheduled execution date for Timothy McVeigh.

Significantly, the Inspector General's report revealed that the destruction of relevant FBI documents was not disclosed to the court, the prosecutors on the case, or the defense until **after** the execution took place. I agree with the conclusion in the Inspector General's report that "the court and defense counsel should have been informed of the FBI's destruction of documents, in addition to being given the belated documents, while McVeigh's stay of execution was being litigated." (report, p. 173). It is unlikely that any of the destroyed documents, if produced, would have changed the outcome of the case, but that does not excuse the FBI's conduct. The observations of the presiding judge in the case about the FBI's conduct are illuminating: He described the FBI as "an undisciplined organization or organization that is not adequately controlled or that can't keep track of its information."(Id., at 131). Yet, in denying the request for a stay of execution, he noted that "It is the function of others to hold the FBI accountable for its conduct here, as elsewhere." (Id.).

This report raises three significant issues for this Committee's review. First, there are structural

and management problems at the FBI which need fixing. You cannot blame a computer or a filing system when senior FBI agents in charge of the Oklahoma City bombing case are aware of document production problems almost five months before the scheduled execution. FBI headquarters officials were also aware nearly three months before the scheduled execution, yet did not disclose these problems to the FBI Director, to senior Justice Department officers, or to prosecutors on the case until a week before the scheduled execution. This appears to be yet another example that the "circle the wagons" mentality has been alive and well in parts of the FBI. When you learn about a problem, you cannot bury your head in the sand and hope it goes away. Efforts to contain a problem under a cloak of secrecy have a tendency to aggravate the problem. This Committee will look to Director Mueller to consider appropriate administrative action against the FBI managers who did not promptly tell FBI headquarters, Justice Department officials, and the prosecutors on the case about the document problems.

The silver lining in the Inspector General's report is the conduct of two lower-level employees, who, in contrast to the managers, did the right thing here. The FBI financial analyst and the intelligence research specialist who first discovered the document production problem in January 2001 promptly informed their superiors in the chain of command, but did not go around them. As the report notes, "the FBI could do well to use this as an opportunity to help remedy a long-standing FBI problem – the belief among FBI employees that bringing problems to management's attention only results in problems for the employee." (Id., p. 139).

Second, the information management and technology problems at the FBI substantially contributed to the belated document production. While we all are relieved that the Inspector General found no intentional misconduct, the report documents a number of fundamental flaws in the handling of information by the FBI that contributed to the failure to produce documents in the Oklahoma City bombing case: "antiquated and inefficient computer systems;" "inattention to information management;" "inadequate quality control systems;" misfiling, mislaying or losing documents by FBI personnel; failure by field offices to follow instructions and respond to leads; inaccurate and misleading communications among FBI offices; and a system and procedures for handling documents that "was -- and still is -- inordinately cumbersome and badly in need of change." This litany of problems is startling, and I am pleased to give the FBI an opportunity today to tell us about what the FBI is doing to address these problems.

We all appreciate the efforts of Director Mueller to correct the management and information management problems at the FBI, and I hope he appreciates the fact that congressional involvement can help achieve constructive change. In the Emergency Supplemental Appropriations Act passed in January, Congress gave the FBI $745 million, with more than $417 million of that dedicated to computer and information technology. Congress is poised in this year's budget process to give the FBI another $245 million. That would amount to a billion-dollar infusion of funds into the FBI, or a 25 percent budget increase since September 11. Just throwing more money at, and granting increased powers to, the FBI, without focusing on and fixing the management and information technology problems that exist, is a certain prescription for future failures – and one that this Committee is no longer willing to write.

Finally, we have to apply the lessons of Oklahoma City to the new challenges facing the FBI in

fighting terrorism. The management and document handling flaws documented in the Inspector General report are chilling and raise the critical question of whether the same flaws hampered the FBI's sharing of counterterrorism information before the September 11 terrorist attacks. It is fair to conclude that the FBI does not know what it knows. How, then, can it effectively analyze or share critical information? That is simply unacceptable when this country faces the threat of terrorist attacks.

Legislative Action Is Necessary

The Inspector General's report demonstrates the need for enactment of S.1974, the Leahy-Grassley FBI Reform Act, to charter the authority of the Justice Department's Inspector General to review allegations of FBI misconduct and to strengthen FBI information management and technology and to protect FBI whistleblowers. Prior recommendations by the Inspector General in three separate reports on information management improvements were not acted upon by the FBI. Our legislation would require the Attorney General to report to the House and Senate Judiciary Committees on steps being taken to implement a 10-point plan for FBI information technology -- ensuring that, this time, the recommendations are not disregarded.

Continued Oversight Is Important

The need for sustained, bipartisan oversight is clear from this week's report as well as from last week's delivery by the Immigration and Naturalization Service of visa confirmations for two of the terrorists who were responsible for the September 11 attacks. The President and the Attorney General recognize the problem, and the Attorney General, yet again, has directed the Inspector General to initiate an inquiry. Judge Webster is completing his evaluation of FBI security in the wake of the Hanssen espionage disaster. Deputy Attorney General Thompson is conducting an independent review of FBI management, and Director Mueller has already started reorganizing the Bureau. We intend to hear from Judge Webster, Deputy Attorney General Thompson, and Director Mueller later this Spring.

Special reports, reform legislation and bigger budgets are important, but they are no substitute for sustained, focused and bipartisan Congressional oversight. That is why Senator Hatch and I have jointly requested additional resources to carry out the Judiciary Committee's oversight duties of the law enforcement agencies whose missions – all the more since September 11 – are so important to the American people, to our civil liberties, to our public safety and to our national security.

# # # # #

STATEMENT OF FBI DIRECTOR ROBERT S. MUELLER REGARDING THE INSPECTOR GENERAL'S REPORT ON THE FBI'S HANDLING OF THE MCVEIGH DOCUMENTS

We commend the Inspector General and his staff for a thorough, objective and independent examination of the issues. The resulting recommendations are constructive and we appreciated the opportunity to cooperate in this endeavor. For some time, we have been making major changes that both implement the recommendations, address the cultural and training issues inherent in a new way of doing business, and address the larger issue of records management as a priority core function.

While we are taking specific actions to address each concern raised by the Inspector general, a number of significant steps are well underway to overhaul our Bureau-wide records management capabilities, to increase accountability for compliance with established records procedures, and to put in place the training and skill sets necessary to bring about full employee "buy in" to a paperless environment. We very much appreciate the support and funding Congress has given to these crucial initiatives. For example:

* We have restructured organizationally to recognize that the creation, maintenance, use and dissemination of our records is a core function that must be fully supported by management as a priority. This has not been the case in past years. Our culture must be committed to automation and our leadership and training must be unequivocally in support of this new environment. To do this:

* We created a Records Management Division to ensure executive direction and full-time over-sight over all records policy and functions, consolidating all records operations to ensure consistency, thoroughness and accountability.

* A professional records management expert, Mr. William Hooton, has been hired from the private sector to run the office. He has been charged with modernizing our enterprise-wide records systems and developing comprehensive, enforceable policies and procedures to ensure records integrity. He also is charged with putting in place those quality control mechanisms that will detect anomalies and problems early on. It is critical that we manage information, not just the systems that support our records.

* Congress has funded and we are implementing extensive agency-wide training aimed squarely at evolving our culture to one that exploits technology in our everyday way of doing business. Leadership for this will come from the top.

* We have retrained every employee on proper document production, maintenance and retrieval and the importance of records management as a core function.

* Basic to any modern system of records is a modern information technology system, and modernization of our information technology is one of our top priorities. We are making sustained progress in this area. Congress has approved funding for the FBI to upgrade technologies and infrastructure for organizing, accessing, analyzing and sharing information throughout the FBI and beyond. Improvements which are currently underway include:

* Replacing the now antiquated Automated Case System in favor of a multimedia and near paperless "virtual case file" with significant improvements in capabilities that greatly reduce the possibility that future documents will be misfiled, lost or otherwise failed to be produced. The new system will dramatically decrease the potential for human error both by automatically doing many functions now done by manual intervention and by substantially reducing the number of opportunities for problems to occur that are inherent in our current systems.

* This new case file document management system, designed with substantial input from street agents, will be of huge benefit by greatly simplifying the records creation and maintenance processes, being user friendly, and by allowing us to manage "leads" far more effectively.

* The FBI's computer network is being completely revitalized to provide a "data warehousing" collaborative environment instead of application "stove pipes." The creation of "data warehouses" and ample supporting networks provide easier and more robust access to and sharing of information and results in integrated databases. The need for ad hoc crisis software applications will be eliminated.

* Private sector support to allow commercial software and professional scanning, indexing and storage of documents to move us rapidly out of the paper environment that was so vexing in the OKBOMB situation.

Sound records management and document accountability are at the heart of the FBI's ability to support investigations and prosecutions with information integrity. There can be no doubt about the accuracy, completeness and proper disclosure of the records we compile during our investigations and used by prosecutors in support of prosecutions.

The ability to maintain, access and retrieve documents is critical to our mission and equally critical to our ability to protect the rights of those charged with crimes. It also is fundamental to robust analytical and information sharing capacities, both functions that we are rapidly enhancing. In short, records management and integrity are core functions that demand the same level attention and accountability as any function we undertake. It must be a part of our culture.

Finally, although his exhaustive investigation found no evidence of any intentional effort to withhold information from defense counsel, the Inspector General's report also criticizes the actions of certain FBI personnel. We are reviewing these criticisms and will quickly move to take any appropriate disciplinary actions.

REFORMING THE FBI IN THE 21ST CENTURY: THE LESSONS OF THE HANSSEN ESPIONAGE CASE

TUESDAY, APRIL 9, 2002

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, Pursuant to notice, at 10 a.m., in room 628, Dirksen Senate Office Building, Hon. Patrick Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Grassley, DeWine, Hatch, Durbin, and Kyl.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning, Senator Grassley, and I have been told Senator Hatch will be joining us.

This is just another in a series of hearings, I think each one, though, of some significance. Since last summer, we have been holding regular oversight hearings on the future of the FBI and sort of the idea of how they prepare for the challenges of the 21st century. Actually, today's hearing is a stark reminder that some of the challenges facing the FBI are as old as the republic. We focus on the role of the FBI as a protector of the highly classified secrets that are really the crown jewels of our national security.

We are, I think, extremely fortunate that Judge Webster is here today. He has a great deal of credibility on both sides of the aisle, credibility that is earned, which is, of course, the best kind. The report by the commission chaired by him demonstrates the vulnerability of the FBI in fulfilling its basic function of protecting our secrets. The American people depend more than ever on the FBI to protect it against terrorism, as we should and as the FBI knows we do, and that vulnerability has to end.

It is this committee's responsibility to ensure the FBI becomes as great as it can be. This series of FBI oversight hearings is an important part of the process, as is the legislation that Senator Grassley and I have introduced to implement many of the FBI reforms recommended by Judge Webster's commission.

The treason of former FBI Supervisory Special Agent Robert Hanssen was a shocking revelation, not only to all Americans, but also to the thousands of dedicated FBI agents and personnel who work around the clock and in far-flung places around the globe to make this country a safer place to live and raise our families. I

know many of those men and women. I know how hard they work. I know the enormous sacrifices they go through, both themselves and their families, and I think how badly hurt they feel by what former Supervisory Special Agent Robert Hanssen did.

I believe Attorney General Ashcroft was right to ask Judge Webster and other outside experts to evaluate the FBI's security programs in light of the Hanssen espionage case. This report is as thorough as it is chilling. The findings are not academic. They have important implications for the FBI's operations in the post-September 11 era.

At least one of the significant deficiencies and security risks documented in the Webster commission report are the result of new policies adopted in response to the September 11 attacks. Unfortunately, these new policies were done without proper consultation with security experts and raise problems of their own.

The commission's findings and recommendations are crucial to the FBI's efforts to fight terrorism and protect national security, as will be the recommendations of the skillful Justice Department Inspector General, who is investigating other aspects of the Hanssen matter for report later this year.

The report is another wake-up call to the FBI, but I worry that when some of these wake-up calls come, the institutional reflex has been to hit the snooze button and that has to change. With the oversight series of hearings which we began last year, we want to help the FBI break the pattern. I blame, to some extent, the Congress. We have taken basically for decades a hands-off policy toward the FBI and not done the kind of oversight that we should do, which is why I began these oversight hearings within weeks of becoming chairman. Working with the Attorney General, who feels that we should be doing it, and the Director of the FBI, who feels the same, and others, this committee wants to help them ensure that the FBI learns from past mistakes and becomes all the Nation needs it to be.

The Webster report exposes within the FBI what the report calls a pervasive inattention to security, which has been at best a low priority in recent years. It describes an FBI where computers so poorly protect sensitive material that the FBI's own agents refuse to put important information on the FBI's official system. It paints a picture of the FBI where employees are not adequately trained in basic document security practices and where there is little analysis of security breaches.

The Webster commission found not one or two problems, but serious deficiencies in most security programs it analyzed within the Bureau, and that when compared with best practices within the intelligence community, "FBI security programs fall far short." It is an FBI security system that does not work, and there are three key findings from that report that we have to look at.

First, the commission found that Robert Hanssen's activities merely brought to light broader and more systemic security problems at the FBI. For instance, Hanssen's ability to mine the FBI's computer system for national secrets for more than 20 years—20 years—points to a serious weakness in information security. Hanssen himself said that any clerk in the Bureau could have done the same, and yet he was promoted to sensitive FBI positions

where he was entrusted with our most sensitive national secrets during a time when he was a paid Soviet spy. That is a problem. His ability to copy highly sensitive material and take it in and out of the building, and nobody stopped him, nobody asked, and nobody followed up.

Second, the commission found that the best way to protect information is not to shut down information flow completely, either within the FBI or from the FBI to outsiders. Indeed, that type of reaction is inimical both to a free society and to effective law enforcement. Instead, the Webster Commission found the FBI needs to do a better job with what is known as defense-in-depth security, find out what is truly sensitive and then protect that.

Finally, and most disturbing, the commission found that the systemic problems which allowed Robert Hanssen to compromise national security for so long are not ancient history but still permeate. Most alarming to me, the commission found that decisions since September 11 have resulted in substantial sensitive source material from FISA surveillance being made generally accessible on the FBI's computers to FBI personnel and then inadequately protected.

This not only presents a security risk which has to be corrected "as soon as possible," but it is the kind of breach that could create some real constitutional problems. We want to be able to prosecute those who are involved in terrorism or playing terrorism against us. Judge Webster knows, a former judge and FBI Director who understands prosecutions as well as anybody in this room, when you get such a prosecution, you want it to stick.

I am afraid that some of these mistakes could allow loopholes to be created where we could not do that and we have to fix that. We have to fix it. We have to make sure that if we are going to be prosecuting somebody, we can make it stick. We have to make sure that we have done enough so that when somebody has sensitive information, they are willing to give sensitive material and know that it is going to be kept that way.

I am one of the ones that helped write the USA PATRIOT Act that gave the FBI new surveillance power and the Webster report raises some very serious concerns in my mind.

I get the impression that part of the Hanssen case, there was a circling of the wagons. Unfortunately, if the enemy is inside the circle, that does not do you much good and we have got to get outside that circle and attack the problems. I think Director Mueller has already taken some steps in the right direction and I commend him for that.

One common sense proposal in the report stands out, establish a system under which security lapses at any one particular agency can lead to improvement throughout the entire intelligence community and thus have a coherent national policy. In fact, the commission specifically cites a proposal for such national security program that I made 16 years ago when I was Vice Chairman of the Intelligence Committee and Judge Webster was FBI Director. We made that report after the horrendous year of the spy, with Walker, Whitworth, Howard, Pollard, Chin, and other spies detected here. So these are things that we should be looking at.

We find that most departments and agencies other than the CIA did not implement the requirements that were adopted after the Ames case. Not much has been done since Hanssen's arrest over a year ago. We do not go into the financial background as they should be. These are things that have to be improved.

Back on the security issue, in 1997, the Justice Department Inspector General's report on the Aldrich Ames spy case specifically warned the FBI needed to develop and maintain a better recordkeeping system for tracking top secret documents, some of the very things Mr. Hanssen later stole. I wonder if then FBI agent and Russian spy Hanssen read the IG report, he knew that he could go on just as he did before, and this would end up in a filing cabinet somewhere. We cannot do that. That is why Senator Grassley and I have introduced S. 1974 to change that.

I have a much longer statement which I will place in the record, but those are some of my concerns.

[The prepared statement of the Chairman appears as a submission for the record.]

Chairman LEAHY. Senator Grassley, do you wish to say something?

STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. I think you said everything that can be said on the subject. I think we ought to take advantage of this opportunity to thank Judge Webster for his excellent and thorough report on these security problems at the FBI. The results of the commission's review are almost painful and I do not think we need to belabor the revelations and problems it found because I think that we are all familiar with them by now.

I would say that this is all the more disconcerting, though, because the FBI missed a number of pretty plain signs over the years that Robert Hanssen was up to no good. Just one of these instances should have sparked a very thorough investigation, the hacking software found in his computer. Yet, even as these instances piled up for more than a decade, no one could connect the dots. This cost the FBI and our nation tremendously. Hanssen was able to sell top secret information that damaged national security and led to the death of several people.

I hope that the FBI works to adopt the recommendations in this report, and I know that the FBI reform bill that Senator Leahy and I have authored will address some of the security issues at the Bureau. I am happy to see the Webster report includes some of the bill's provisions, and just one of them would be the establishment of a cadre of career security professionals.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Did you wish to say anything?

STATEMENT OF HON. MIKE DEWINE, A U.S. SENATOR FROM THE STATE OF OHIO

Senator DEWINE. Mr. Chairman, very briefly, I just want to thank you for holding this hearing, and Judge Webster, it is good

to see you again. We appreciate your service to our country and your continued service with this very, very good report.

Mr. Chairman, I am looking forward to Judge Webster's testimony and the testimony of the other witnesses. I would just make one comment before we start, and that is that these recommendations will do no good if they are not implemented, and these recommendations will do no good if they are not funded. I think we kid ourselves if we did not realize that this was going to cost money.

It seems to me that the followup, the logical followup to Judge Webster and his commission's good work is for the FBI to very quickly do the cost analysis and to come to the U.S. Congress, come to the American people and be very, very candid and say, this is what it is going to cost. You make the decision as far as public policy, but we need to acknowledge that this is what the cost is going to be, because if we do not do that, we are not being honest with ourselves, and quite candidly, we are never going to be able to implement the recommendations that the Judge has made.

So I thank the Judge, and Mr. Chairman, thank you.

Chairman LEAHY. Thank you very much.

Judge Webster, the floor is yours.

STATEMENT OF HON. WILLIAM H. WEBSTER, MILBANK, TWEED, HADLEY AND MCCOY, LLP, WASHINGTON, D.C.

Mr. WEBSTER. Thank you very much, Mr. Chairman. Thank you for the opportunity to testify before the committee on behalf of the Commission for the Review of FBI Security Programs. I am going to keep my opening remarks brief because the commission's true statement is its report, which I have submitted and which you have.

In March 2001, Attorney General John Ashcroft asked me to chair the commission at the request of FBI Director Freeh. The request came in the light of the newly discovered espionage of FBI Special Agent Robert Hanssen. Over the course of 22 years, Hanssen gave the Soviet Union and Russia vast quantities of national security information of incalculable value.

The depth of Hanssen's betrayal is shocking, but equally shocking is the ease with which he was able to steal classified material. Usually, Hanssen collected the material during his normal daily routine, gathering up classified information that crossed his desk or arose in conversation with colleagues.

The commission concluded that internal security has often been a low priority at the Bureau, frequently trumped by operational needs. Security training has been almost nonexistent and agents usually take on security duties as collateral responsibilities with every incentive to return to investigative operations full time.

Although it is impossible to eliminate intelligence efforts directed against our national security, the commission attempted to recommend changes in FBI security programs that will minimize the harm those who betray us can do. The changes should also shorten the time between the defection of these individuals and their detection.

Most globally, the commission recommends that FBI security programs be consolidated in an Office of Security, reporting to the

Director. In addition to changes in Bureau policy, we also recommend that a system be established whereby security lapses in a particular intelligence entity lead to improved security measures throughout the entire intelligence community.

Mr. Chairman, I would like to acknowledge the support afforded by the Department of Justice and the unstinting cooperation of FBI Director Mueller and Bureau personnel at all levels. The commission also noted the many steps the Bureau has taken to improve security in the light of Hanssen's treason.

Finally, I would like to recognize the dedication of our professional staff and my colleagues on the commission, the Honorable Clifford Alexander, the Honorable Griffin Bell, the Honorable William Cohen, the Honorable Robert Fiske, the Honorable Thomas Foley, and the Honorable Carla Hills.

At this point, Mr. Chairman, I would like to depart from my formal statement to add a few words of my own on a personal note and then I would be happy to respond to your questions.

I am painfully aware that some of Robert Hanssen's activities took place intermittently when I was Director of the FBI, and while I worked hard to strengthen its counterintelligence capabilities to detect and capture the spies of hostile countries targeted against us, in hindsight, I took our own internal security procedures for granted and I share in that institutional responsibility. In fact, I raised that issue when I was asked to assume this responsibility and was assured that my perspective from 9 years at the FBI and four-and-a-half years at CIA would be useful.

So with the authority of the Attorney General, I asked six distinguished Americans of unquestionable probity to serve with me as commissioners, and they have joined me in the conclusions of this report. I wanted this to be an honest report, and I believe that we have produced one.

This report, Mr. Chairman, is not intended to reflect adversely on the integrity and dedication of the many thousands of men and women who have served their country in the FBI. Indeed, its purpose is to disclose the security vulnerabilities that could have been far more devastating had not the spirit of fidelity, bravery, and integrity been alive and well for all but a minute number of employees who betrayed their trust.

I think we owe it to the men and women of the FBI who serve today and will serve tomorrow to address these vulnerabilities in ways that will best protect our country and yet permit the FBI to function fully and effectively in its many responsibilities for the protection of us all.

Now, Mr. Chairman, I would be happy to respond to your questions.

Chairman LEAHY. Thank you very much, Judge Webster. Incidentally, that statement is also typical of your own candor and the credibility you have established in this town.

Senator Hatch has joined us, and traditionally, I do want to give him an opportunity to make an opening statement.

STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Senator HATCH. Thank you, Mr. Chairman.

I want to commend you, Judge Webster, for the excellent work you have done every day you have been in this town in so many ways and especially for your findings and for your work here. Again, everybody in this town knows that you are a person of immense integrity, and so are the others who have worked with you on this report.

But over the course of the last year, we have become acutely aware of the damage that FBI Special Agent Robert Hanssen has done to our national security. Over 22 years, beginning in 1979 and continuing until his arrest in 2001, we are told that Hanssen gave the Soviet Union and Russia substantial amounts of vital information affecting the United States security.

When Mr. Hanssen's activities were discovered, we all questioned whether his ability to jeopardize our nation's security was due to deficiencies in the FBI's internal security. Commendably, Attorney General John Ashcroft and then-Director Louis Freeh responded quickly to the crisis by appointing Judge William Webster to lead a thorough and independent review of the FBI's internal security programs.

This commission has now completed its task, and it is apparent from its extensive, well-written report that the commission was very meticulous in its investigation. The Webster Commission's comprehensive study will guide the FBI as it undertakes the critical task of transforming its internal security programs.

I want to commend you, Judge Webster, the commissioners who served with you, and your staff for diligent work in compiling this report. I want to acknowledge in particular George Ellard, who was Senator Biden's chief counsel on this committee for his service as general counsel on this commission. Our nation owes a debt of gratitude to Judge Webster and the members of his able team for their dedication and for their thorough and important review.

Reforming a multi-faceted institution like the FBI is no easy task. As the Webster report points out, an inherent tension exists between the Bureau's law enforcement function, which is grounded in shared information, and its intelligence function, which, by necessity, must be grounded in some degree of secrecy. Conflicts between operational and security objectives are common. The recommendations contained in the Webster report appear to strike a workable balance between these obviously competing objectives by advocating reforms that will increase the Bureau's security without jeopardizing its efficiency in the law enforcement area.

I am pleased to learn that under the leadership of Director Mueller, and immediately before him Director Freeh, the FBI has examined its security programs and has already incorporated many of the security reforms the Webster commission has recommended. Most significantly, the FBI has established an independent security division led by an assistant director whose role is to plan and implement the FBI's security programs. As the Webster commission suggested, consolidating the FBI's security functions into a central office will not only increase the Bureau's focus on security matters, it will also ensure greater security coordination within the FBI.

In addition, the FBI has improved the security of its information systems, instituted frequent polygraph examinations and access reviews, and developed a comprehensive security education aware-

ness and training program. So we look forward to the FBI continuing to incorporate all of the reforms recommended by the Webster commission, as the Bureau has indicated it will.

I want to take a moment to commend Director Mueller and his team. Director Mueller has been on the job only 7 months, and during virtually his entire tenure, he has been coordinating the FBI's response to the September 11 attacks. I am sure I am not alone in my admiration for the institutional reforms Director Mueller has already managed to accomplish under these trying conditions and circumstances. I believe, as a newly installed Director, Mr. Mueller should be allowed to implement his reforms, and as I know he is aware, to be accountable for the results.

As I have said on countless other occasions, the FBI is one of the finest law enforcement agencies in the world. We have learned, however, we cannot let our respect for the FBI as an institution or for the many hard-working agents who are often asked to put their lives on the line blind us from the fact that the FBI has, on occasion, come up short of our expectations and that, indeed, is a serious matter.

We must keep in mind, however, as the Webster commission has noted, the FBI is not the only governmental entity that has been betrayed by one of its trusted employees. The General Accounting Office has reported that between 1982 and 1999, 80 Federal Government and contractor employees were convicted of espionage. That is an astounding number. As the Webster commission observes, with the exception of the Coast Guard, since the 1930's, every U.S. agency involved in national security has been penetrated by foreign agents. In this information-driven age, the FBI and all governmental entities must learn from their own mistakes and from those of one another to ensure that our nation's security is not jeopardized and that it is protected.

I applaud Director Mueller for the significant steps he has taken in his brief tenure to address the FBI's security shortcomings. I have the utmost confidence that he will continue to capitalize on the Webster commission's study to improve the Bureau's security programs. In the months ahead, I look forward to hearing more about the FBI's progress, and I am convinced that under the able leadership of Director Mueller, the FBI will remain the world's standard in law enforcement.

I want to pay special tribute to our committee chairman for holding these hearings and for showing the great interest that he has in these matters. This is important stuff.

Again, Judge Webster, I just want to thank you on behalf of the American people for all the work you have done through all these years and for all the help that you have given this committee through all these years and for all of the great suggestions that you have made, not just in this report, but in the past, as well. You have been a real asset here in Washington and in our country and I just wanted to personally pay my own personal tribute to you.

Mr. WEBSTER. Thank you very much, Senator.

Senator HATCH. Thank you, Mr. Chairman.

[The prepared statement of Senator Hatch appears as a submission for the record.]

Chairman LEAHY. Thank you.

Judge as you know, the Leahy-Grassley FBI Reform Act has a number of provisions on FBI security. One creates an FBI security career program. Another authorizes counterintelligence polygraph screening with, I think, pretty good safeguards against misuse. The third formalizes improved pay for the FBI police force that guards its buildings. The fourth requires a report to Congress on FBI's computer security. And a fifth, and this is something that Senator Grassley has spent years emphasizing, provides enhanced whistleblower protection in the FBI.

Would these provisions be helpful in carrying out the kind of recommendations you have made in your report?

Mr. WEBSTER. Mr. Chairman, I believe that all of those suggestions which are incorporated in your bill offer promise for greater security and greater attention to security and greater understanding and training of security within the FBI. If I am not mistaken, I think there is also a passage asking the Inspector General of the Department to make a recommendation to you with respect to whether he or someone reporting to him should function as a special Inspector General for the FBI. I do not know the answer to that one, but I will follow that with a great deal of interest.

Chairman LEAHY. Thank you. The USA PATRIOT Act gave the FBI new electronic surveillance powers, some very significant, many of which will sunset in 4 years. I raise this because obviously the question of whether they sunset or not is going to depend upon how they are utilized. I made clear, though, at the time of the passage that this committee is going to have to do some very extensive oversight of how these laws are carried out.

Your report actually is one of the very first chances for an independent body to evaluate the FBI in the post-September 11 situation, and your report talks about the FBI's decision to place highly sensitive FISA, or the Foreign Intelligence Surveillance Act, information on the computer system. This is a system that is generally, as I understand, accessible to all FBI personnel during the same time as they were telling Congress they want to be entrusted with more powers under FISA because the information would be kept so close held and so specific that we could allow an expansion in FISA, this very extraordinary type of wiretap and search authority, something that we have allowed only under very limited carve-out.

The FBI asked for more of it, saying this would be kept very, very closely. And yet, we find that they have put a lot of that on the computer system that just about everybody in the FBI could get hold of.

You gave them a poor grade in handling that. First, you say that the FBI's action under September 11 presented a security risk to FISA information, which should be corrected as much as possible. And second, even though it was not the focus of your commission, which you said had a couple of circuit judges on it, former Attorney General, former U.S. Attorney, independent counsel. You are a former U.S. Attorney, circuit judge, FBI Director, and CIA Director. You criticize the FBI's handling of FISA material because it raises potential issues of constitutional law and, therefore, could hinder the Bureau's ability to construct cases that could be prosecuted.

I have a lot of prosecutors that tell me, and I happen to agree with them, that we want to get these terrorists. We want to pros-

ecute them. We want to convict them. But we do not want, because the procedures run foul, to see the case get thrown out.

So what has been the reaction of the rest of the intelligence community to the FBI posting of FISA information in this kind of a data base?

Mr. WEBSTER. Mr. Chairman, I cannot really speak for the reactions of the other members of the community other than my understanding that those who were interviewed expressed some concern and dismay with what happened.

I am going to speculate now, which is always a dangerous thing, but I think in the period immediately following September 11, with the desire to try to come to grips as soon as possible with what was behind all of this and the people who are responsible and what other plans there might be, there was an effort to get information out, including FISA information, without the people with the best of motives having fully consulted the security people for the possible consequences of putting that material into the automated case system where it was available to everyone.

The FISA statute has been extraordinarily useful on behalf of the national security and intelligence community and for prosecutions, when appropriate. I have to confess that it was passed just about the time I arrived in Washington and Attorney General Bell wanted me to come up and talk to you in support of it and I was not sure that this statute was necessary. I thought there was an implied authority in the President to protect our national security by ordering electronic surveillance of those who are suspected of espionage or of acting in a hostile way to the United States.

I have since been convinced it was a great statute. It is serving a very useful purpose. But it needs to be protected. That information contains affidavits, the whole process of getting an authority to conduct a national security warrant, especially after the Keith opinion required warrants in the case of domestic security cases in 1972. The "t"s have got to be crossed and there has to be great care and a lot of very sensitive information is contained in the material that goes into the Justice Department, as you said, and is presented to this special court for authorization. But then to find it suddenly turned loose and put in the huge file where it is available to other people represents some serious potential problems.

I think that my own conclusion is that had we had a security division in place, had we brought them to the table on this issue and listened to their advice, we would have done it differently.

Chairman LEAHY. In fact, that is really my point. If you had the security division, they could say, look, we want to do this. We want to get this information out as quickly as possible. What are our parameters? How do we do it? That is the important part to me, because everybody wanted to get any other terrorist who might be in this country, or potentially in this country. We had a devastating attack. We wanted to protect ourselves against it. We wanted to get the people responsible. Obviously, some were dead, but we wanted to get anybody else involved with that. We knew that there had to be more. Just instinctively, you knew that we faced more attacks and that there were more people available, so you wanted to do that, but you want to do it in such a way to protect your assets and you protect your ability to get a conviction.

If we were in a closed session, there are cases—I am sure you can think of some, and we would probably be thinking of some of the same ones—where FISA has been extraordinarily helpful to us, but in getting the information, if that is made public, it would be very obvious just where it was we got that information and that door would close so fast.

Mr. WEBSTER. That is right.

Chairman LEAHY. We would take forever to replace it. For example, suppose Robert Hanssen had been able to access FISA information right from the computer on his desk. I think it would be pretty obvious to everybody there would be an enormous amount of damage he could have done.

So I think the idea of having—and I agree with you—the idea of having a security division or procedure where you could just go and say, look, we have got a lot of information here, what can we use, what can we make accessible, and what—do we have to follow certain procedures in who is going to have access, I agree with you.

Mr. WEBSTER. Mr. Chairman, implied in what you have been saying and what I think I have been trying to say is that sometimes, people who make these authorizations do not really understand what putting something into the ACS system means and that is where security comes in.

Chairman LEAHY. And I do not question the motives. Everybody wanted to get—we all had the same motives. I think the Nation is probably as united as any time I have seen it in public life. It was united to find who did this and to get them. But for those who are going to be prosecuted, they want cases that can stand up. For those who are going to have to continue to mine sources that we had for the coming years to protect us, they did not want those sources to go away. That is what we have to be protective of.

Your report recommends the FBI submit an initial report and a report annually for 3 years on how they plan to address and fix the security programs. The House and the Senate Judiciary Committees have primary oversight jurisdiction over the FBI in general and over criminal espionage cases, such as the Hanssen case in particular. Should we be getting that report that you speak of, for the FBI submitting an initial report and a report annually for 3 years on how they plan to address and fix these security programs? Are the House and Senate Judiciary Committees the appropriate places to receive that report?

Mr. WEBSTER. I think so. We may have said to the intelligence community and intelligence committees, and I think that is a matter between this committee, which has worked so long with the FBI, to work it out.

Chairman LEAHY. They should have it, too, but——

Mr. WEBSTER. We think it is important that the Congress be in the loop here, and Senator DeWine said something we may come back to, but understanding what is needed and the costs can be very important as the use of electronic filing and electronic techniques becomes more the order of the day and we are seeing less documents and more things put in a computer system that perhaps in the past has addressed security after the fact. You should be part of the process of making sure that the money is available, that the FBI is not starving for modern technology, which is, as you

know, changing every two or 3 years. If they are changing every 10 years, it is not going to work.

Chairman LEAHY. I have young agents telling me that they are looking at equipment that was antiquated when they were in grade school or high school——

Mr. WEBSTER. That is right.

The CHAIRMAN [continuing]. Being used there, and they just almost have to go back and learn how to use it, and if it is that antiquated, it does them no good.

My last question is this. You talk about that the FBI does not have a viable program for reporting security incidents to headquarters. Now, on paper, they are supposed to report these, but we found some very chilling stories from whistleblowers that people are afraid to report security lapses because they are afraid it is going to hurt their career. I know one employee reported a security violation and ended up basically getting hounded out of the job for it. We have to have better whistleblower protection, do we not?

Mr. WEBSTER. I think so. I think the whistleblower protection that you provided for will be very useful in answering that problem.

Chairman LEAHY. Thank you.

Senator Hatch?

Senator HATCH. Thank you, Mr. Chairman.

Judge Webster, we are all too aware of the circumstances, or should I say the numerous and significant security breaches that have occurred in almost every government agency. You have recommended in your report and again here today the creation of a system that will enable officials in one intelligence agency to learn from the mistakes of the others and the successes of the others, as well.

I share your view that such a system is critical and long overdue, but would you elaborate a little bit on such a system, on how such a system will operate and who would participate in such a system and how would their findings be communicated to the relevant and appropriate agencies?

Mr. WEBSTER. Senator Hatch, we were purposely general in our recommendations there. We see a very clear need to share experiences so that there can be a top, a standard level of quality, and whether that is through the Director of Central Intelligence or some other vehicle, we did not attempt to decide in our recommendations.

I am reminded that shortly after I undertook this responsibility, representatives of the Central Intelligence Agency came down to tell me about a number of the things that they were doing because I knew that among other things we would have to confront is whether or not the FBI needed to have a vetting procedure which, from time to time, would check on the people who were in sensitive positions to be sure that they were still everything that we expect of special agents of the FBI. The CIA had a long ongoing polygraph vetting program. The FBI did not. It did not have any when I was there. Director Freeh put in place a process for polygraphing prospective new entrants to the FBI, but there was no vetting process.

So I wanted to know more about it, and when they came down to talk to me, I thought it was interesting that they said, "We do

not want you to make the same mistakes we made," and they had reference, I am sure, and then they said so, to the 300-odd agents that were put on hold, because ghost special officers with their careers on hold because of problems in the polygraph examinations that they took. They recommended that we have a more discreet, refined kind of vetting process that the agents could be comfortable about, that would know was necessary, but they were acknowledging they have made mistakes and here are some of them.

I think, in answer to your question, there has to be a forum where those issues at the security level can be acknowledged and this is what we did about it, or another agency can say, here is what we recommend that you do because we had the same experience. It is as simple as that.

Senator HATCH. Thank you. As I stated, I am most encouraged by the steps that the FBI has already taken to implement some of——

Mr. WEBSTER. Yes, they have.

Senator HATCH [continuing]. Some of the reforms recommended in your commission's report, and I am pleased to learn that the FBI intends to institute all of the commission's recommendations or suggested reforms. Recognizing that the implementation process will require both resources and time, are there any particular areas of improvement that the FBI should accord top priority?

Mr. WEBSTER. I suppose each of us would have probably a different priority list. My first priority is to see that security division come together and be effective, and I would hope that they would have direct access to the Director. At this stage, I believe that they have access to an executive assistant director. In order to signal the importance of the division, I think they should have access to the Director, and out of that security division can come a number of other programs.

I put training at a high level because there really is not much training in security outside of the National Security Division, and I think that is a process that is easy to build into the ongoing training programs.

Looking at specifics, the information systems that are in the FBI, which are in the process of overhaul, are very important to the future of these programs and the future of the FBI's ability to function well. I would hope that some of the problems we have identified—and incidentally, this report refers to some 22 appendices which are still classified and they go into great depth about some of the technical problems. Some really are over my head, but I understand the problem. I would hope that in the information security area, continued attention be given to building in and responding to these security issues.

I am concerned that Robert Hanssen was able to make copies of about half of what he was able to deliver to the Russians and the Soviets without anybody noticing or caring about it and he was able to walk out the door with them. He was also able to walk out the door with individual documents. But I believe that it is a smaller point but very important that copies of classified information are just as classified as the original documents and the procedures have to be worked out to limit the ability of people to wander over

to a copy machine and make several copies and not be accountable for them. So there is a certain level of accountability there.

Financial disclosure should be implemented in the FBI. They are not burdensome. We have all done this. I think you all have done them. I know I did them as a government officer and they provide a vehicle for looking for anything that would suggest that someone is engaging in activities or receiving compensation from some unknown source. Those are part of the vetting process.

The polygraph is important. The FBI's program is more ambitious and aggressive than the one we suggested, but we suggested what we thought was a minimum which could be easily accommodated to a changing culture and a changing realization that polygraphs are not that intrusive. I took one when I was Director of the FBI and I took another one as Director of Central Intelligence and I understand why they are necessary. I understand their restrictions. But I think that is important to build it in.

I also believe that we should not act on just a polygraph alone. We should act on the polygraph plus—plus other evidence of aberrational behavior, that we should not take people offline and subject their careers to perils because of some blip in the polygraph process.

I suppose that if I had my druthers, I would be trying to see what more could be done to enhance the reliability and capability of the polygraph. I do not see much evidence that a lot of money has been spent to improve something that has been around for 20 to 30 years. Since it does have problem areas, I would say let us try to address them, but not give up an important tool.

The vetting process is a means not only of detecting activity but of deterring people from the temptation to sell out their country when they know that the chances of their being detected more than simply on entry into the agency are there.

So those are some of the things. I know I have neglected other things. Document security, personnel security, information security, and structural solidarity are key to it. But I have always felt that when we have a problem, as we did in the Keith case, which resulted in the 98 agents who had been engaged in "black bag" jobs under what they thought were lawful procedures back in the 1970's, came from not properly informing the agents themselves and educating them. Neither the Department nor the FBI told them about the Supreme Court decision other than to close all the following case due to a Supreme Court decision.

Since that time, it seems to me training is important. If you tell special agents what the problem is and what is expected of them, they are the most responsive people on earth in doing their duty as they understand their duty. They need to understand and be trained in the importance of security.

Senator HATCH. Thank you so much. I appreciate your service.

Chairman LEAHY. Thank you.

Senator Durbin of Illinois, and then we will go to Senator Grassley.

STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Senator DURBIN. Thank you very much, Mr. Chairman, and thank you very much for joining us today, Judge Webster.

I think one of the things that struck me as I got into this issue was the whole question of computer technology at the FBI. I will have to say that as a result of an oversight hearing, what was it, the first in 10 years or more with this committee that Chairman Leahy sponsored, I was really just amazed at how bad it is—how bad it was.

We brought up Mr. Dies, who was in the process of trying to update the computer technology at the FBI, and his report to us was really startling in terms of the inadequacy of the computer resources at the agency, and he identified for us some obvious things which, as a person in the private sector, he was stunned to find, and that is that there is no e-mail at the FBI—at least, there was not as of a few months ago, no access to the Internet. The whole security aspect of this thing was obviously open to compromise, as Hanssen proved over and over again.

Now, I know that there is an effort underway, Trilogy, to make a dramatic change in this, and it is my understanding that some offices have already started to update the equipment and such. But as you got into this, what was your findings in terms of the adequacy of computer resources in addition to the security aspect? For us to criticize the INS for sending out a visa to someone who was a terrorist on September 11 is one thing, but for the FBI to be unable to communicate even within its own agency, let alone to the INS and other agencies, about dangerous individuals raises an even larger question. What did you find?

Mr. WEBSTER. As I said before, Senator, a good part of the appendices deal with the shortcomings and we have identified those on a classified basis, so if I speak in general terms to you, I would say that, primarily, the computer automation of data programs have been under-financed for years. There is so much evolution in the computer world today that it is strange to me to think that when companies are getting new equipment and new procedures every two or 3 years, that the FBI would go for 10 years trying to get along, limp along in an area where data was coming in at them from all directions and from other agencies sharing information with them and they did not have a proper place to take care of it.

The Trilogy program was an effort to kind of pull themselves out of the swamp and to deal with what they had, to add to what they already had, and to look for what they needed in the future, but I am not satisfied that that is going to be enough. I think there needs to be a Congressional partnership here in making sure that they have the funds and that those funds are spent wisely and well. Put security right in there at the beginning of the architecture.

Senator DURBIN. Let me just make this a matter of record. I agree with you, and after September 11, I kind of picked this as my favorite project. Let us try to update the computer technology at the FBI. I contacted Director Mueller as well as the Attorney General's office, the Vice President, and Chairman Leahy spoke directly to the President about this. We were prepared to create some

waiver situations so that they could obtain updated technology there and not be hamstrung by our procurement process. We were stopped by the OMB. The OMB says, no, no, we do not want to see that happen. There are ways to do this. There are ways to accomplish it.

Now, this was 6 months ago, and I said at the time, all right, prove it. Come in with the technology. Do it on a timely basis. Bring this kind of information technology and the security associated with it that might stop people like Hanssen in the future.

Well, I have not heard back, but I will tell you a number of us are very frustrated that what we thought was a good faith effort to give to the FBI the tools and weapons they need was thwarted by another Federal agency of this administration. We cannot expect to win the war on terrorism fighting with muskets, and when we do not have computer technology at the FBI up to the job of worldwide and global terrorism so that it can be a proactive force and security in place so that we can stop the likes of a Hanssen in the future, then, frankly, we are going to diminish our capability to protect America.

Mr. WEBSTER. I could not agree with you more, Senator. One of the areas that has been near and dear to my heart, in response to Senator Hatch's question, I guess I did not really mention it, but in the computer world, it would seem to me that we need more trip wires and that they have the ability to do that, trip wires that would identify someone who is off the reservation.

We used to have, back in my primordial days, we used to have librarians who would recognize the fact that someone was asking for a file, who was asking for something outside their range of business and would report it. We need electronic librarians and ones that not necessarily just go to the case agent. They have that capability. A case agent can look and say, "Who has been looking in my case file?" But it would go to a part of the security apparatus who could quietly take steps to find out, was there something going on here?

Senator DURBIN. Did that not happen in the Hanssen case, where he, in fact, compromised the password of one of his superiors and gave as his excuse that he was setting up some new technology and the superior did not even report it, really did not——

Mr. WEBSTER. Something like that. There were a lot of capabilities that Hanssen had identified that he could do. Really, he was not a hacker because he did not need to hack. He had access to the crown jewels and there was no vetting process to see whether or not that was—but these electronic trip wires, it seems to me, appropriately place watching guard over the more sensitive files, would be useful and important. They cost money, but I think that they are important.

Senator DURBIN. Well, when you consider Hanssen's damage to America, it is certainly worth the investment to put these in place. Do you feel, had they been in place, that we might have detected his activity at an earlier point?

Mr. WEBSTER. I think that is true to a degree. Unfortunately, I call him my 500-year flood. He was positioned unlike most every other special agent. That was his job. He was in an area where he had almost unlimited access. Therefore, in his case, I think the

likelihood of detecting it sooner would have been through a vetting process.

Senator DURBIN. Let me ask you this. Do you feel the culture at the FBI can change?

Mr. WEBSTER. Oh, yes, I do.

Senator DURBIN. Do you think the mentality, that J. Edgar Hoover-Elliott Ness mentality of the past, the fortress mentality, do not look inside, this is our kingdom, do you think it is open now to change along the lines that we have been discussing?

Mr. WEBSTER. I certainly do. I think we have all been chastened by this experience. It is a matter of training. It is a matter of understanding. And then, OK, that is it, let us make it work. That has been my experience throughout my 9 years.

Senator DURBIN. I think the same of the new Director and I hope he can achieve that.

Thank you, Mr. Chairman, and thank you, Judge Webster.

Chairman LEAHY. Thank you. I might note, Judge Webster, Senator Durbin has strongly pushed for a long time for not only increased funding, but better computers. He has done it with the Vice President. He has done it with the President. He has done it with Director Mueller and Attorney General Ashcroft. And, of course, he is right. Bob Dies, who has come here and testified, has emphasized that, the necessity to improve it.

The way of just checking it, a lot of places have a thing that if you use a pass key to go into a room, it logs in that it was you and the time and everything else. It is relatively easy to do the same. We do it on our computers and everything else, who went in there, and then have the people with appropriate security constantly checking who went where when.

The vast majority of people are very honest within the FBI. They would not be there if they were not honest and dedicated. But it is like having the two warehouses full of goods. One has got locks on it and an alarm system and one has unlocked doors. The crime is the same to break into either one of them and steal things, but you know which one is going to get broken into.

Senator Grassley, again, a person who has spent an enormous amount of time on this subject, and I appreciate your taking the time from your other committees to be here today.

Senator GRASSLEY. Thank you very much.

Once again, we thank you for your report, and I think your report makes very clear that we are never going to be able to eliminate all espionage attempts against the United States but that we ought to have as a goal, quite obviously, to make it more difficult to spy and easier to catch the spies.

Now, Hanssen was a spy at the FBI for 20 years. Aldrich Ames was one for many years at the CIA. During these periods of time, directors came and went at both of these agencies. You even had your tenure during this time. Yet, it took so long to detect them.

Based on your expertise and your background in intelligence matters, is there anything outside of your report that we can do to detect these spies earlier? I ask that question in the chance that not every idea you considered is in your written report.

Mr. WEBSTER. Senator, one thing I would say on the side, because it is not technically an issue of security, which was our

charge here, I think it is ironic that almost every spy that we have found, both at CIA and at the FBI, has been found with the aid of recruited sources of our own in other hostile intelligence agencies who have given us a lead that we have a problem. The numbers that were listed by the chairman, not only the names that were listed by the chairman, almost all of them, I think perhaps all of them were found because we had an aggressive program of human intelligence recruiting assets on the other side.

We do not want to neglect that just by trying to lock up our equipment. We have got to continue that capability and build on it. You will not always get very much information. In Pilton's case, or Howard's, we called him "Bob," but we went from a series of things with little bits and pieces to find out who that person was. Pilton was 9 years later that we got the information, but Howard earlier, and so on. So I would say, let us not neglect our human intelligence development in the interest of security.

Vetting, to me, and by that I mean periodic assessments. The background investigations must be taken seriously. I have had the sense over the years that sometimes because of the high level of trust that existed between special agents, they were more perfunctory than they were real. I go back to what President Reagan used to say, "Trust, but verify." If you do not, you are going to have long periods of time.

Hanssen never took a polygraph. He was never really subjected to a serious background investigation or a financial disclosure. Somewhat the same in the case of Ames, and they were so backlogged over there that I think there were anomalies that were not detected in the course of his examinations.

So we have to do things in the more sensitive areas of the FBI to be sure that the people on board are still on board and the kind of people we thought they were.

Historically, sadly to say, as I look back on the record of espionage in the United States, treason, these were volunteers. I had a conversation with a KGB general and a man who was his former residente in Moscow after the end of the cold war and wanted to know what did we think about their capabilities against us, and I said, well, your trade craft was excellent, but you should not take a lot of credit for recruiting because in almost every case that I know of, the American was the one who picked up the phone and made the contact or wrote a letter or took the initiative.

We have to know when someone is of that frame of mind before he has had an opportunity to do damage, or at least to catch him as soon as he tries it. We can watch, and we do watch with our matrix systems very closely hostile intelligence service activities in the United States to see if they make contact, but that will not work in every case. We have to have a vetting process to which officers and agents willingly submit, and so it must not be demeaning. It must be a logical way of protecting ourselves, just as drug testing is the order of the day for people who deal in drugs, and that is not intrusive, in my opinion, as long as it is kept that way. People understand its necessity.

That leads me to one of perhaps my biggest question marks in our report that I think has to be thought through, and that is this. Not everything in the FBI—in fact, the majority of what is done

in the FBI does not involve sensitive national security issues. If we were to impose the same level of security on the entire operation of the FBI, we would be in danger of slowing this locomotive down to an unacceptable level.

And so there has to be a way of looking at classified information that relates to our national security that is different than classified information that is maybe called "secret" but is purely law enforcement in nature, has nothing to do with our national security issues. And we have to have a way of building a circle around those who deal in our most sensitive things and they have to be willing, for the trust that is given to them, to accept some additional intrusion on their private life.

But to do that routinely for everyone in the FBI, I think represents a cost and impediment. I wish I had a quick and easy formula for this, but I think it is there. I think it can be drawn and I think that the computer systems and the access and the need-to-know issues can be focused primarily upon those who have the access to this kind of information we have been talking about this morning.

Senator GRASSLEY. Let me followup on the last point you made. Your report revealed that after the Paris attack last year, senior FBI officials lifted restrictions on access to information in the Bureau's computer systems. Some of this information was FISA-related, which obviously is highly sensitive. I am sympathetic to the need to share information, especially during times like this, but my primary concern here is that some of this information might betray the sources or methods used to obtain it. In your opinion, how much is at risk if FISA information is shared?

Mr. WEBSTER. Senator, I think there is substantial risk of damage here. The affidavits that are offered in support of FISA applications for electronic surveillance can disclose the names of the sources of that information, many of whom are valued assets of this country and whose identity, if disclosed, could result in personal damage or death to them and loss of important sources of information to us.

I just do not think security was sufficiently at the table when that decision was made. There was a rush to get information out and I think that perhaps people who made the judgment did not fully understand the ACS system and what that meant in terms of easy access and availability of information, and this information was allowed to float up into it. I am sure that in the future, the first question will be what can we put out for everyone that will not damage our national security or our important sources and our important methods.

Senator GRASSLEY. My last question is maybe a little too cynical, but do you think government agencies are destined to only fix internal security after a spy is found?

Mr. WEBSTER. That seems to be the wake-up call, historically. This is a unique opportunity, I think, to build security into the automated systems, to build it into training, to make sure that the work is valued and respected, and we have not talked enough—I think one of the Senators this morning, members of the committee, talked about providing a career path in security for the FBI. I think that is necessary, but I would also say that security goes out

into a lot of field offices where they may not be able to support a large security presence but there has got to be an effort made to have that work valued.

If people see it as an impediment to their career or are asked to do it on a collateral duty basis or for a time-being basis, they are apt to think, if they do not value the work and appreciate its importance, they will think that I am being shunted off to something and it is going to affect my career and I do not want to do it.

So we need people who, just as in the Justice Department, who provide outstanding services in security. We need to have people in the FBI who see that as their career and also are able to train and make aware other special agents of the importance of their work. It needs to be respected, and I think that the words "pervasive inattention" is a fairly accurate assessment of what it has been up to now, and I include myself in that category. It needs more attention and that is through training and awareness and respect for the career possibilities that good security work can produce.

Senator GRASSLEY. Thank you. Thank you, Mr. Chairman.

Chairman LEAHY. Senator DeWine?

Senator DEWINE. Chairman, thank you.

Judge your commission report, I think, raises an interesting question, and that is can a law enforcement culture, which is really grounded in the sharing of information, coexist with an intelligence culture, which we all know is really grounded in secrecy, not sharing anything and compartmentalizing everything.

The British do not seem to think so. They, of course, have Scotland Yard domestic law enforcement, but they have split the internal and the external security between M5 and M6. Do you think we should consider doing that with the FBI, in other words, splitting the law enforcement and the intelligence functions of the FBI?

Mr. WEBSTER. Well, I think it is always fair to consider it, but my own pretty well developed judgment on it is that that would not be a good idea, and if I may explain. We have field offices all over this country. Most of them are dedicated to primary law enforcement. But from time to time, as in New Mexico, for example, for Edward Lee Howard and others, you are going to find national security issues.

I think it is important that the National Intelligence Division be sufficiently staffed to be able to deal with problems throughout the country. If you started building a whole separate organization, I suspect that we would be starved somewhere along the line, in unable to fund it or the administration would not support that kind of funding.

Canada tried it. It has not done well in Canada. When it was part of the RCMP, I think there was far much more ability to find things, track things all throughout Canada, and I would go slow on that.

But you came very close to what I was talking about earlier. I would find a way of building a wall around the information and the data that is collected for national security purposes so that that information was subject to the highest level of security and that you did not attempt to impose that on the entire FBI, where we had a very substantial risk of people who say, this is nonsense. This is slowing us down. We do not need this.

We need security throughout the Bureau, but if we can find a way to flag the kind of information that we are concerned about, the kind that Robert Hanssen was delivering to the Russians, inside the Bureau, I think that is the answer.

Senator DEWINE. I think that is an excellent answer. Basically, you are saying we need some way internally to flag it, to wall it off so that it does not create problems on both sides of the wall.

Mr. WEBSTER. Exactly.

Senator DEWINE. I would like for you to put your hat back on as former Director of CIA. As I understand it, the DCI has the authority over the rules and regulations regarding classified information, whether that information is being held within the CIA or the FBI. What has been your experience as far as how often or how well the DCI actually utilizes that authority and is there a way to improve that?

Mr. WEBSTER. My impression is that they are using that authority more effectively today than I did when I was Director of the CIA. There is a tendency—we have all gone through periods—I had five-and-a-half years in the Navy in World War II and the Korean War and had responsibility for taking care of classified information aboard ship. After a while, it tends to be burdensome, particularly if you are busy. It is important that those rules be understood by people who can then interpret them to the people within whose agencies they work and that they be as clear as possible and that they not be so technically difficult that the special agent on the street cannot understand them and, correspondingly, will not try to understand them.

Senator DEWINE. But you believe that the DCI is utilizing that authority more today than historically?

Mr. WEBSTER. That is my impression, because we are in a kind of war right now and I think it is important that that be done.

Senator DEWINE. Just post-September 11, though?

Mr. WEBSTER. Well, I think it was going on before that. The outreach to the community has been stronger. There have been, as you know, the counterintelligence function that I started in 1988 is headed by a representative of the FBI so that the FBI has its role in this process, as well. But the agency has always had a big security effort and the DCI orders, I believe they are called, or DCI rules are coming out more regularly now than I remember them.

Senator DEWINE. Judge, I want to conclude by getting back to something I said in my opening statement, and that is that the next step, I believe, is for the Bureau to do a cost analysis of your report. When you were doing your report, how much did you factor in cost and were you cognizant of that? You had a lot of experts there. I know you did not do a dollar-for-dollar cost analysis or item-by-item cost analysis, but that had to be somewhere in the back of your mind.

Mr. WEBSTER. It was, and most of the appendices—not most, but a substantial number of the appendices have to do with not only the capability but what is involved in maintaining them. I do not know that we have any specific costs. We have some clear statements from people we interviewed and our own conclusions that the FBI has been woefully starved in this area.

There has not been a real voice for change. The FBI is one of the most thrifty organizations I have encountered in American government. They try to get along with what they have, but they need a lot more than they have been given and they have not really made their case loud enough for people to understand how badly they have needed it. It has been a kind of "get the truck working again," as I think we say in the report.

Senator DEWINE. I think your report makes that case loud and clear and your testimony does, as well.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Kyl?

Senator KYL. Thank you, Mr. Chairman. I would like to put my statement in the record, if I could.

I would just ask one question of Judge Webster so that we can move on to the next panel. I have been watching on television and I have read your statement and part of the report.

Turning from the Hanssen case to another that has concerned me, the Wen Ho Lee case, that is a situation in which virtually every governmental agency involved—in fact, I think I can say every governmental agency involved—made significant mistakes. The cumulative effect of which was to prevent an adequate investigation and prosecution, in my view, and the FBI was a part of that.

One of the concerns with respect to that case was at least as far a I am concerned, the disconnect between the field office and main FBI headquarters. The inability to share information back and forth because of something, I do not know whether it is directives, it is tradition, or what, and I would like your comments on the recommendations with respect to integrating better the information at the national headquarters with information in the field offices and working together as a team on investigations. Rather than the situation which seems to me to have pertained, which is the local field offices doing their thing, in many cases, unconnected to the national office, and both of them know something about something but neither knows what the other knows or knows that they know it, and, therefore, investigations are compromised. Could you comment on that, please?

Mr. WEBSTER. Senator Kyl, I agree with that observation. I served on the National Commission on Science and Security from the Energy Department following the Wen Ho Lee case and we saw enormous examples of differences in culture and attitudes and between scientists and law enforcement officers and others trying to come to grips with what was important in that case.

I have a better example, I think, of what you are talking about in some of the post-9/11 period, when people in New York were reluctant to put their information into the ACS system because they knew that then it was available to anybody. Whatever the motivation, besides good security, that might have been there, teamwork, the term you use, is vitally important if these things are going to succeed, and sometimes getting the information to headquarters will make sure that headquarters recognizes something that is bigger than or more involved than the local field office has seen. But

the field office has got to trust the system at headquarters in order to make sure it does not hold things back for whatever reason.

Senator KYL. Could you amplify with respect to your commission report what you recommend in that regard to bridge this gap, to overcome this problem?

Mr. WEBSTER. Well, it was a rather complicated thing that I do not think we have in the FBI because they had to deal with the scientists' desire to know and share and the security effort to protect our national resources. There, they came to a kind of risk assessment. How much risk is there? That has some value in the law enforcement in the sense that if you rate the risk unreasonably high for everything, people will stop paying attention to it and that is sometimes a problem, as well, when people say that is nonsense.

In fact, some journalists suspect in the military that things get classified just to cover mistakes. I do not think that is really the case in many cases, but there have been enough situations to warrant that kind of feeling about it.

There has to be a rational approach to how people share secret, top secret, information and how they make sure that people who have an interest in it get a chance to see it and draw that judgment. Some of the problems with the FBI, there are a number of cases which have attracted criticism that have involved one person knowing but not telling or not sharing and, consequently, something not getting done.

Another example over at CIA—I do not mean to criticize them, but the whole issue of the bombing of the Chinese embassy, if you recall, in Central Europe. Some people knew that that was a Chinese embassy and not something else, but the people making the maps and the targeting did not know.

The dilemma that needs to be addressed, and it can be addressed, is how do we keep from giving it to more people than need to know but be sure that people who have a rational need to know do, in fact, get it.

Senator KYL. Well, is the answer not to necessarily have headquarters put out a bulletin to all district offices or field offices saying, "look, we have a problem in this regard," but rather to insist on knowing what is bubbling up from down below? Going back to the Wen Ho Lee case, again, the national headquarters had certain things it was trying to look for. The local office, the field office in Albuquerque was doing certain things and they were not talking to each other and part of the problem with that whole investigation was that lack of connection.

Are there recommendations and are there changes being made to address that problem, and if so, what are they? Do you know?

Mr. WEBSTER. Well, I think that the appendices, which are classified, do contain that level of recommendation. We think that in terms of security as distinguished from investigations, we have addressed it in the recommendation for formation of a security division. The National Security Division has a responsibility for making sure that on national security issues, local field offices are appraised of what is going on and expected to return information in kind for analytical purposes.

On pure law enforcement, I would hope that there are not too many cases where headquarters does not know about significant

developments. I do not think we want to run law enforcement from headquarters, but we have to have, as you say, that interchange of information. The big problem is this enormous amount of information flowing into the automated case system without any real control over what happens to it, who sees it, its reliability, and so forth.

Senator KYL. I want to thank you. Thank you, Mr. Chairman, for holding the hearing and the attention you have given to this, as well as Senator Grassley, and Judge Webster, again, for your continued great public service. We appreciate it very, very much and look forward to visiting with you more on this.

Mr. WEBSTER. Thank you, Senator.

Chairman LEAHY. Thank you, Senator Kyl. Before we started, I told Judge Webster that every time he tries to retire from public service, we do not let him. We keep bringing him back.

In fact, the day before your report was made public, the FBI had also issued a report about what they have done to improve security. Were you able to compare what they have done and what you have recommended?

Mr. WEBSTER. I was. I think, in general, they have moved on and listed the things they have already accomplished. Throughout our investigation, we shared what we were learning and where we were going and no attempt to hold back. This was a serious thing that the FBI needed to get moving on. We wanted to have a report that was in depth. We looked at all the facts and here they are, and in some cases, I anticipated there would be no surprises and there were not.

They have moved even more aggressively on the polygraph route. They have indicated in some of their materials things that are not accomplished but planned, things that are coming forward. I think a substantial number of those are contained in our report and I am glad to see there is very little air between us on what needs to be done. The important thing is that the Bureau move on it.

Chairman LEAHY. And I think that is important. I realize you were not asked to go through the FBI's counterintelligence investigation, for example, in the Hanssen case, but just taking what is in the press, I mean, you talk about places where there were warning signs that should have come up. After Hanssen began spying for the Russians, his wife's brother raised concerns about his sudden affluence. Another FBI agent told the security office that he thought Hanssen's wife was getting money from her family.

As brought up by several here, Hanssen hacked into his boss's computer and then claimed he was just testing the system. I do not have anything classified on my computer. Several of us have to handle classified material all the time, and if we do, we go to the special committee room where that is. But if I found somebody hacked into my computer in my office, they would have one heck of an explanation they would have to do.

He was caught using a password break-in program. He was suspended for a week because of a physical encounter with an FBI employee. He took a stripper girlfriend with him on an inspection trip to the FBI office in Hong Kong. He was known to persistently seek information beyond his normal need to know. He had official knowledge of the Felix Block espionage investigation before Block

was somehow tipped off. An internal FBI study recommended looking for Russian penetration inside the FBI, but that was dismissed. Both the FBI and CIA focused their investigation on the CIA rather than on FBI personnel with similar access.

There are a lot of clanging bells. It is easy in retrospect to go back and say, oh, my gosh, look at this thread. It is like reading the mystery novel and in the last paragraph, somebody sits up and says, but do you not remember that, and that pulls it all together. But, unfortunately, it is not just a novel you put down and you pay $25 for it. It is something that we are ultimately going to pay hundreds of millions of dollars for.

I do not mean that as a question, Judge, but I think it is very wise what you have done, and in the electronic age, where you do not have a file that is locked up in a cabinet somewhere, you have a file that is suddenly on every single laptop in the Bureau if not handled correctly, I think it is very important.

I appreciate very much your responses on the issues of FISA, which I think is a major one of concern to prosecutors and others, and I think you have given very good warning to the things that should be done. We all want to catch a terrorist, but we also want to make sure that we can catch them next year, too, and not just now, and that we can stop them in the future.

Senator Hatch, unless you have something further, or anybody else on the committee——

Senator HATCH. I think we have kept the Judge long enough.

Chairman LEAHY. I am glad this committee does not have to do the normal billing from Milbank, Tweed, and I say that somewhat facetiously, Judge, but just again, the country benefits by your willingness to take on these kinds of activities and I thank you very much.

Mr. WEBSTER. Thank you, Mr. Chairman. If I may say, I am very grateful to the commission members and to our staff. They did a wonderful job. All of us felt it was a privilege and an honor to be helpful and we hope we have been.

Chairman LEAHY. Thank you.

[The prepared statement of Mr. Webster appears as a submission for the record.]

Chairman LEAHY. We will take a 2-minute recess while they reset the table.

[Recess.]

Chairman LEAHY. Thank you very much. First, I will put the Webster Commission report in the record. It will be included as part of our record, something I should have done before.

In this panel, Mr. Szady and Mr. Senser will be testifying. Mr. Watson will be here. We are going to go to 5-minute rounds.

I would note Senator Kyl raised a totally appropriate question. I believe that Mr. Szady is going to testify that he is centralizing all the espionage cases in one section, which should help address the problems that Senator Kyl raised, appropriately raised, about the Wen Ho Lee case.

Mr. Szady, you are on, and I appreciate you also being here. You have heard all of Judge Webster's testimony. Certainly, if there is something you want to add to that, feel free.

I would also note that, following our normal procedure, you all will see the transcripts of your testimony. If there are items you feel you should have added or want to elaborate on, we will make provisions so you can do that. This is to be helpful not only to the Senate Judiciary Committee, but also hopefully to help the whole Senate.

Mr. Szady, go ahead, sir.

STATEMENT OF DAVID SZADY, ASSISTANT DIRECTOR, COUNTERINTELLIGENCE DIVISION, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. SZADY. Mr. Chairman, if I could, on a personal note, I doubt if many people in here know where Winooski, Vermont, is, but it is a pleasure to testify before a fellow Michaelman.

Chairman LEAHY. What year, Mr. Szady?

Mr. SZADY. Nineteen-sixty-six.

Chairman LEAHY. You are just a few——

Mr. SZADY. Just a few years after you.

Chairman LEAHY. You are a youngster. Thank you.

Mr. SZADY. Mr. Chairman and other members of the committee, I would like to express my appreciation to you for inviting me to share my thoughts and provide with you an update on changes we are making to the counterintelligence program at the Federal Bureau of Investigation.

I am pleased to be appearing jointly today with Kenneth Senser, Assistant Director of the FBI's recently established Security Division. By necessity, the cooperation between our two divisions is complementary and seamless. Our Director is committed to protecting the full range of U.S. national security interests and has made counterintelligence, along with counterterrorism, and prevention his highest priorities.

Because the world has changed so dramatically, the FBI is making significant changes to its counterintelligence program. Our end goal is to more effectively and efficiently detect, prevent, and disrupt hostile foreign intelligence activity directed against the United States and its interests. The FBI appreciates your support as we continue to implement these changes across our organizations.

First, I would like to provide a very brief assessment of the characteristics of foreign intelligence threats of the 21st century, for they provide a basis for understanding our new national, centrally managed counterintelligence strategy.

The United States faces an intelligence threat that is far more complex than it has ever been. The threat is increasingly asymmetrical as it seeks to exploit the areas where there is a perception of weakness within U.S. national security approach and organization. Traditional notions of counterintelligence that focus on hostile foreign intelligence services targeting classified national defense information simply do not reflect the realities of today's more complex international structure.

Foreign targeting of the elements of national power, including our vibrant national economic and commercial interests, continues to evolve. While traditional adversaries were limited to centrally controlled national intelligence services, today's adversaries include not only these traditional services, but also non-traditional and

non-state actors who operate from decentralized organizations. Moreover, the techniques and methodologies used to target classified and sensitive and commercially valuable proprietary information march forward with the advance of technology.

This new environment and the uncertain future that accompanies it present the FBI with new challenges. The FBI's role as the leader of the nation's counterintelligence efforts requires that we understand all dimensions of the intelligence threats facing the Nation and match them with new, innovative investigative and operational strategies. The FBI must continually assess and measure its performance against ever-evolving threats found in these new and different environments.

The constant parade of new technologies, the vulnerabilities created by them, the extraordinary value of commercial information, and the globalization of everything are but a few examples. The FBI must focus its resources on those actors that constitute the most significant intelligence threats facing the nation, wherever that might come from, and in all of these new arenas.

In response to the increasingly complex intelligence threat environment, the FBI is taking measures that reorient its counterintelligence strategy, prioritize intelligence threats, and make the requisite organization and managerial changes to ensure U.S. national security interests are protected. The following initiatives are underway.

We recognize that in order to mitigate the intelligence threats our country is now facing, we must continually redesign our counterintelligence program. Historically, when the threat lines were more clearly drawn, counterintelligence at the FBI was largely decentralized, with field divisions setting local priorities and assigning resources accordingly.

To effectively recognize and counter the extremely diverse intelligence threats now evolving, a new more centralized and nationally directed, focused, and prioritized program is more effective. By centralizing our program, we will ensure the ability of the FBI to be more proactive and predictive in protecting the critical national assets of the country. Centralization cements accountability regarding counterintelligence program direction, control, and leadership. Moreover, a centralized counterintelligence program facilitates the FBI's cooperative and collaborative interaction with other members of the United States intelligence community. The counterintelligence environment must be transparent.

Our national strategy will be totally integrated with the Office of the National Counterintelligence Executive to ensure that our efforts are focused on policy-driven priorities and that we are positioned to protect identified critical national assets. Our efforts will also be seamless with the CIA to ensure that our counterintelligence efforts extend worldwide.

As part of this nationally directed strategy, I have undertaken a comprehensive strategic planning effort that is providing the FBI with the framework in which to prioritize and address intelligence threats. This framework is based on community-wide analysis and direction and recognizes that there can never be unlimited resources, so we must be focused on the greatest threats. This will

better position the FBI for the future by changing our performance expectations, management practices and processes, and work force.

The central elements of this initiative are development of clear strategic objectives and operational priorities in support of those objectives; a highly trained and specialized counterintelligence work force with a management team that reinforces counterintelligence as a specialized priority career within the FBI; a much stronger operational component within the Counterintelligence Division, to include a stronger program management; an ongoing system of accountability that clearly defines responsibility for all elements of counterintelligence; an enhanced communication strategy that is more effectively communicating counterintelligence policy, plans, and priorities; and greatly enhanced analytical support that relies more extensively on a highly specialized discipline is necessary.

Accepting responsibility to prevent and disrupt foreign intelligence threats and espionage from threatening U.S. national security requires the Counterintelligence Division to adopt a more proactive posture. One organizational change that I have made consistent with this goal is the establishment of a Counterespionage Section within the Counterintelligence Division from existing base resources. This new section is responsible for managing all of our major espionage investigations. The section evaluates and prioritizes all existing espionage cases.

In order to meet the challenges ahead of us, I am ensuring that the most important resources the Counterintelligence Division has, its human resources, have the appropriate tools available to effectively implement our mission. While the FBI has historically provided counterintelligence training to new special agents, we now need a systematic approach to a comprehensive counterintelligence training regimen applicable throughout the agent's career. We are studying this training program and will implement it shortly. Agents and analysts assigned to work counterintelligence should have a systematic and integrated training program.

Analysis, as I said, is another area of my focus. Counterintelligence analysis is central to our program, to ongoing investigations and operations. I think today's challenges require much greater reliance on and bringing in much greater numbers of outside subject matter experts, also, to bolster our efforts in understanding.

Information management and intelligence sharing are also two areas that we are improving, in concert with the directives established by Director Mueller regarding these subjects. The technology being put in place at the FBI will vastly increase our capability to maximize the value of what we know, and even more basic, to know what we know. These new technologies will be the thread that ties the community together.

In summary, counterintelligence and counterterrorism are the FBI's leading priorities. If we are to successfully mitigate the asymmetrical intelligence threats facing us today and in the future, a new approach, new ways of thinking, and better technology are required. We are in the process of redesigning the counterintelligence program at the FBI. It will be much more centralized to ensure the program is nationally directed, prioritized, and that appropriate management and accountability measures are in place. The Coun-

terintelligence Division will continue to work closely with the Security Division to ensure that our activities are complementary and that the FBI is able to comprehensively address any internal threats.

Through our ongoing comprehensive strategic planning process, we are ensuring that our counterintelligence priorities, performance, expectation, and management practices are designed in a manner that is responsive to ensuring our national objectives. We are working to not only ensure that counterintelligence personnel have the best possible tools to conduct their work, but also to enhance the training and experience among counterintelligence personnel and to bolster counterintelligence as a specialized and vital career within the FBI. Thank you.

[The prepared statement of Mr. Szady appears as a submission for the record.]

Chairman LEAHY. Mr. Senser?

STATEMENT OF KENNETH H. SENSER, ASSISTANT DIRECTOR, SECURITY DIVISION, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. SENSER. Good morning, Chairman Leahy, Senator DeWine. Hopefully, I will not be forced to tell you what I was doing in 1966.

I spoke to you initially in July——

Chairman LEAHY. You piqued my curiosity, but no, you will not be forced to tell.

Mr. SENSER. Thank you. I spoke to you initially in July of last year to discuss our assessment of the FBI's security program and the need to transform this program into an operation capable of addressing the diverse and formidable threats facing the Bureau. I am very pleased to be back in front of you today to give you our update on the progress in that matter, but also to commend Judge Webster for the extraordinarily thorough and helpful product that he and his commission provided.

As I discussed in my testimony last year and as highlighted in Judge Webster's report, the security program at the FBI is in need of critical reform. Suffice it to say that every element of the security program requires improvement in some form or another. On a positive note, we have made substantial progress in the last year, but make no mistake that an incredible amount of work is still required. Very smart people are going to need to take time to carefully formulate and implement these reforms.

I also testified during my July testimony that prior to Hanssen's arrest, the FBI identified seven areas that required critical and immediate focus. Thanks to Judge Webster, we have received recommendations that provide us with specific and sound guidance in each of these critical focus areas.

Within my statement for the record, we identify in some detail the specific accomplishments we have made, as well as those initiatives we plan on making. I have described these in somewhat of a generic format in order to avoid giving our adversaries a more detailed plan of our countermeasures, but I am prepared to provide the committee with a more substantive briefing in a closed session.

Immediately after Hanssen's arrest, the FBI initiated some interim security enhancements that we had discussed in July, specifi-

cally, the limited expansion of the polygraph program, the use of more extensive auditing in our automated case support system of those persons accessing the most sensitive FBI files, the establishment of an enhanced reinvestigation analysis capability, and some more generic enhancements designed to facilitate a change in the Bureau's culture relative to security, and also to elevate the role of security at the FBI.

Since July, we have made a number of other noteworthy changes, to include, for example, in December of 2001, establishment of the Security Division, for the first time in the history of the FBI, having somebody responsible as the Director of Security operating at an assistant director level and with access to Director Mueller in order to bring forward issues of concern.

We have also initiated the comprehensive review of security policy and have begun to build a foundation for a comprehensive security education, awareness, and training program. We have taken significant steps in building a robust information assurance program, hopefully to address many of the issues cited by Judge Webster in his report. And we have also improved the vetting that is done to establish trustworthiness, both initially and on a continuing basis for our employees. Finally, we have taken steps to more tightly control the information that is present in hard copy documents at the FBI.

In summary, we intend to deliver not just a series of manuals and policies, but to effect a dramatic adjustment in the security culture at the FBI. Continuing security education, widespread security awareness, and making security an accepted and normal part of everyday business is our challenge.

As I have already mentioned, this is a long-term effort. We will continue to carefully examine those recommendations supplied by Judge Webster and his commission and will carefully study the classified appendices that he referenced. In addition, we will also review the Department of Justice Hanssen study that we expect later this year in an attempt to evaluate their recommendations and ultimately build a stronger action plan.

Mr. Chairman, Senator DeWine, I appreciate this committee's support and the support of your colleagues that you have provided to the FBI so that we are able to faithfully discharge our duty and do what we can to protect the interests of this great nation. Thank you.

Chairman LEAHY. Thank you very much.

[The prepared statement of Mr. Senser appears as a submission for the record.]

Chairman LEAHY. I have had, actually, indirectly some discussion of this, but I will go directly and I will ask this of Mr. Watson. After September 11, we realized there is a lot of material, odd documents and even some electronic surveillances that had not been translated. I had asked both Attorney General Ashcroft and Director Mueller to go back and review things that were available to us and to them prior to September 11, not to destroy anything that just because it may have been sent may have been overlooked. But the Director even went on TV, issued a plea for translators. Some of these languages, you find in kind of a small community here in this country, a fairly close-knit community often, who speak the

language. Some may even have ties to foreign governments. So if you are in a crunch, you have got to hire them on the one hand. On the other hand, you have an obvious security concern. Judge Webster mentioned this in his report, on page 58.

What is the FBI now doing to check and do security and monitoring to make sure that we do not, in our need to get these translators, we do not get somebody that could create a bigger problem than the solution they might give us?

STATEMENT OF DALE WATSON, EXECUTIVE ASSISTANT DIRECTOR FOR COUNTERTERRORISM/COUNTERINTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. WATSON. Senator, that question, I guess the answer lies into the system that we have in place to make sure, one, the need to get the information translated, as you well pointed out, as well as the security balance, and there is a definite security procedure that individuals go through in order to be hired as a translator. There are some conditions where we can pick up contract employees that are not going to be permanent FBI employees but still have the security risk. There is always a balance there of being able to get the information that we have collected translated and weigh out those considerations with individuals that are going to translate that material.

Since 9/11, we have made some progress in that area and that is definitely a priority, not only with us, I know with all the other intelligence communities and we are working closely with the security folks to make sure that we do not bring someone in that translates it and steals it at the same time.

Chairman LEAHY. The Webster report talked about the self-policing that can be done on these things. FBI employers or contractors, if they learn of a violation, just come forward and report it. But then you get some concerns where that is seen as whistleblowing and it actually gets discouraged. Do you feel there is more they can be doing to encourage people, if they think that there is a security violation, to come forward and report it?

Mr. WATSON. Yes, sir, and we have—which the Director is fully aware of and fully supports, that employees, if they detect inappropriate activity, security violations or unethical activity, that they have an obligation to report that, and there is a mechanism set up to report that. I know you and Senator Grassley are concerned about that, is that being done, but I can say that with my experience in the Bureau and I think with Mr. Szady's, I mean, I am not sure of any instance where anybody would look the other way on a security violation or a matter of ethics or a criminal violation that should not be reported.

Chairman LEAHY. We may want to followup on that privately——

Mr. WATSON. OK, sir.

Chairman LEAHY [continuing]. But let me ask Mr. Senser, you referred to the commission's report as a road map for the FBI, but you also say some of the identified vulnerabilities are more critical than others. Is the FBI going to accept everything that is in the report or what is going to happen?

Mr. SENSER. When I mentioned that some of these vulnerabilities were more critical than others, I was referring to a prioritization that has taken place in the sense of trying to address those gaps that could pose the most damage immediately, for example, the gaps in our information system security, where large elements of the population may have access to very sensitive information, and certainly establishment of this robust information assurance program is at the top of our list as one of the initiatives that we are trying to move forward very quickly.

In addition, from a prioritization standpoint, the education and awareness of our employees, as Judge Webster mentioned, making sure that people understand at the beginning what the proper way is to handle materials and how sensitive they are. I also believe that in most cases, people want to do the right thing and if they know what that right thing is and understand it, then they will be more apt to comply.

Then in addition to that, this security violation process and making sure, again, from education and awareness, that people understand where to go with their concerns and that there is a mechanism for centrally addressing them, tracking them, and taking action on them.

Chairman LEAHY. Mr. Watson, I am not going to ask Mr. Senser this because he cannot give himself a promotion, but Judge Webster and the commission would like to give him one. They would like to recommend elevating the position of the Security Director to a status that reports directly to the FBI Director. Is that a recommendation being considered by you?

Mr. WATSON. Yes, sir, and I think that has been proposed as the Security Division, and I would like to say that one of the things in the commission report was making security a priority. I can tell you from the operational side that we view that as a critical piece, in view of the Hanssen matter, and we fully support that and as a full partner and taking considerations in for security as well as what we are trying to do operationally.

Chairman LEAHY. I am going to give you a couple of questions for the record, but I want to make sure that both Senator Grassley and Senator DeWine have a chance to ask questions. I have some other questions for all of you.

One area, and you have heard us talk about it a great deal here, is the question of material that may be FISA-related material. I cannot underscore how much attention I want given to this. We gave the FBI some very expanded powers, but assuming that with those, that there are some very, very strict ways of keeping track of the information. FISA has been a very helpful tool in going after terrorists, but I cannot think of anything that would more quickly destroy the ability to use FISA than to have the information spread all over and into places where, on the one hand, our own constitutional safeguards should not go, but then second, from our own intelligence security places it should not go because so many times it is going to be sources and methods. Without going into specific cases, if we were back in a secure room, you and I could come up with some of the exact same ones, you cannot let these go out.

So I will have a specific question on it, but please, if you are doing any debriefing back at the home office, you can tell them that

I am very concerned, and I know several others are, on this FISA issue. We want to help. We want FISA to work. But, boy, the rules have got to be followed.

Mr. WATSON. Senator, we are committed to following the rules and we understand the sensitivity of FISA information and how to protect that and that is a vital piece of our investigative efforts, and we thank you for the PATRIOT Act and what you allowed to do. Just let me reassure you that we are not wholesalingly throwing out FISA information.

Chairman LEAHY. I understand. I just want to make sure that we do not do it in such a way that it, in effect, is sitting there in the box where people can take it, I mean the electronic box, and——

Mr. WATSON. We understand.

Chairman LEAHY. No, I am not suggesting you are, but you and I could both look very quickly at some of this FISA material and know, just looking at it, it should not go any further. But if it is out the door, there are others who might not look at it that closely.

Mr. WATSON. That is understood.

Chairman LEAHY. Senator Grassley?

Senator GRASSLEY. I thank you very much. Mr. Senser, the first couple of questions I am going to ask you deal with the timing of your changes which just came out, and then I want to ask you about some of the things that you are planning to do that are not done yet. This is from your remarks.

The question that is most on my mind is why it took until just last week for the FBI to announce so many reforms and changes for better security. The announcement, Wednesday of last week, was timed 1 day before the release of the Webster report.

I have two issues. First, can you or anybody else here from the FBI answer why the Bureau did not learn from the mistakes of other agencies with spies, and why could the FBI not have years ago put in security measures across the board like other agencies did, like expanded polygraphs, looking at employee finances, and better document security. In fact, in regard to employee finances, I believe that Mr. Hanssen himself said if they had been put in place, that would have caught him. So that is my first question.

Mr. SENSER. I think your question is a very good one relative to why the Bureau did not adopt the recommendations that were made as part of the Ames case or Pitts or the other prior espionage cases, and obviously not being an FBI employee, I cannot specifically answer that question.

I can tell you that I have gone back and listed those recommendations that came out in those previous cases and mapped the initiatives that we are planning and have accomplished against those recommendations to ensure, in fact, that we are going to take those into consideration. In fact, I have had a matrix put together, not just of the former espionage recommendations, but of all recommendations that have come out, both on internal studies and external studies of which we are aware, in order to ensure that no recommendation has gone unreviewed.

In terms of the timing of the enhancements, as I mentioned, shortly after Hanssen's arrest, former Director Freeh initiated a number of interim security improvements, and essentially, we have

not stopped since then. This has been a continuing process of making changes as we can, things that were within our purview, and steps to improve the security posture. As Judge Webster mentioned, we have worked very closely with the commission and his team in order to ensure that we were going in the right direction and that the things we were contemplating and proposing were not off track. So we have been working very carefully to try to keep this on a parallel track, not just waiting until the commission issued their report, but trying to move ahead with reforms and enhancements as the commission did its work.

Senator GRASSLEY. Then could I ask the purpose of the press conference last week, if all this was going on parallel to the report? I guess I asked the question. What was the purpose of the press conference, then?

Mr. SENSER. The purpose was to simply make a positive statement as to the steps the Bureau was taking relative to security.

Senator GRASSLEY. I guess I see it as kind of a preemptive strike, but let me go on to the next point, and this is in regard to the number of security measures that are under the planned part of your prepared remarks from last week, called "Transforming the FBI's Security Program." Could you tell me how many of these planned security changes were planned before the FBI received the Webster report?

Mr. SENSER. I would say—I would like to say all of them. I would say 99 percent of them. As I say, this is—I like to think of this as a joint effort between the commission and myself. Obviously, they did not share with me the nature of their recommendations per se, but we have had a very close relationship over the 13 months of their work and bounced lots of ideas off each other in terms of where we were headed.

Many of these initiatives that we have proposed are included in our fiscal year 2003 budget submission in order to try to obtain the funding and the resource levels needed to actually effect these changes. So most of this has been on the record for some time.

Senator GRASSLEY. The Webster report paints a scary picture of the FBI where almost anyone can access almost any kind of information on the computer system, where insiders can get right out of a building with top secret papers, and where no one could connect the dots on Robert Hanssen's spying. I realize that many of the security reforms will take some time to take effect and really make a difference and others are still on the drawing board, but when we see this, we fear that the Bureau's security measures are not yet in place to catch a spy. We learned from the Hanssen case. Now, that is not saying that there is a spy in the FBI because I do not know that there is, but there is real concern about a gap until security is up to speed.

How certain are you about the FBI's internal security right now? Would a spy be detected, do you think, with the things that have taken place?

Mr. SENSER. I think we are still at substantial risk relative to what we have to do, and again, this is going to be a period of time that we are going to have to build expertise and put the infrastructure in place to really support the kind of effort that is needed to successfully bring the matter under control. I would say certainly

that with a lot of the things we have done, such as the expansion of the polygraph program, that there is a greater possibility that if there were somebody operating inside the FBI today, that there is a better chance of detecting them than there was a year ago. But certainly, I cannot say with certainty that that person would be detected.

Senator GRASSLEY. Mr. Chairman, I think what I am going to do is submit two questions for Mr. Senser for answer in writing.

Chairman LEAHY. Thank you. In fact, I will keep the record open for at least 24 hours so that member Senators who have conflicts today can submit questions.

Senator DeWine?

Senator DEWINE. Thank you, Mr. Chairman.

Mr. Senser, the Webster Commission report characterizes the Bureau's existing computer system, and I quote, as "an old car broken down in a ditch." Congress allocated $379 million in November 2000 for the FBI's Trilogy initiative, but the commission says this sum will merely get the old car out of the ditch, not provide the Bureau with state-of-the-art information systems. How much more funding do you think is needed to provide the FBI with the state-of-the-art information systems?

Mr. SENSER. Well, I think there are——

Senator DEWINE. Short-term and long-term?

Mr. SENSER. Right. I think there are two issues there. One is the issue of this state-of-the-art information system, which I would have to defer to Bob Dies relative to business needs from an information technology standpoint.

The second part of that question, though, deals with this robust information assurance program. The FBI received as part of our counterterrorism supplemental roughly $56.7 million to begin the process of building an information assurance program. We are currently working with the appropriations staff to deliver a—well, actually, we have delivered, but we are working with them on the spending plan for that money so that it can be released and that we can move forward on that.

That is the initial investment in information assurance, but it is going to take outyear investment, as well, both from the standpoint of maintaining the improvements we have made as well as adding some additional improvements, and there are moneys in the fiscal year 2003 intelligence request for some capabilities that will assist us greatly in building the kind of program that could have potentially detected a Hanssen, the kinds of things such as auditing, real time intrusion detection capabilities, and so on.

So, again, we have a very ambitious plan on the drawing board and it is going to take support into the out years to make that happen.

Senator DEWINE. It seems to me that the burden is on the FBI to tell this Congress and to tell the American people what it is going to take, and that is obviously a continuing burden, once we are beyond the publicity of the report and today's headlines, because these systems obviously are not built overnight. They are not maintained overnight. They are not improved overnight. So I just assume that the FBI is going to continue to do that.

Let me ask you this. Is there anything in this report of substance that the FBI disagrees with?

Mr. SENSER. No. I mean, the fact is, as I said, that we are very appreciative of the work of Judge Webster and the commission and while certainly there are semantic differences, perhaps, in some areas——

Senator DEWINE. Right.

Mr. SENSER [continuing]. But the substance of the report is solid and we are working hard to address these issues.

Senator DEWINE. Have you done a total cost analysis? You talked a little bit about, or a great deal about the cost, but have you done a total—has the FBI sat down and said, OK, this is what this is going to cost? You have not had much time to do that, but——

Mr. SENSER. Yes.

Senator DEWINE [continuing]. As far as the report is concerned.

Mr. SENSER. Right. As I mentioned, we prioritized our approach to this knowing that time was of the essence. Once we identified—in fact, we had identified those seven critical focus areas I mentioned prior to Hanssen's arrest, but subsequent to his arrest, we built a prioritized approach that outlined 15 categories of enhancements that we felt were critical to pursue. Because of the, again, the fact that there was not much time, we staged those enhancements to get to the most critical, or get the most critical into our fiscal year 2003 budget request, and as Director Mueller had testified in front of the Appropriations Committee, that 2003 request for security totals around $78,065,000.

In terms of the big picture, however, we recognize that many of the things that we are going to have to explore, we are not going to know the full extent until we really get some people on board with the expertise that can look at it. Again, the Webster report will help us considerably there, but there are areas in the physical and technical security realm as well as the police protection side that we are going to be building into our 2004 request and beyond.

Senator DEWINE. One last question, Mr. Chairman. Mr. Senser, my understanding is the FBI has not, as of this date, complied with Executive Order 12968. This is the order that requires Federal employees and contractors to complete financial disclosure forms. Is that correct?

Mr. SENSER. That is correct.

Senator DEWINE. Are there plans to adopt this disclosure and monitoring program, as the commission's report recommends?

Mr. SENSER. Absolutely. In fact——

Senator DEWINE. Do we have a time table on that?

Mr. SENSER. Well, one of the things that Director Mueller did shortly after coming in was, as part of his internal reorganization of the FBI, looked at internal resources that could come to the security program and identified a number of positions that ultimately were sent to security. Of those, there is a number of positions, five, in fact, that we have identified to form the basis of this financial disclosure program. We are advertising now for people that have the kinds of skills in financial analysis that will allow us to develop the foundation.

We have also spoken with other intelligence community members as well as the Department of Defense and their personnel security research people that have a fairly solid foundation in financial disclosure programs. So there is very definitely a plan.

We are also working with the policy coordination committee structure as part of the NSC and one of their subgroups who is dedicated to actually establishing financial disclosure programs within the executive branch, because, in fact, there are a number of agencies, as well, that have never adopted this requirement and we are going to be a part of the effort.

Senator DEWINE. Do you have a time table?

Mr. SENSER. I would like to have something in place within the next 6 months in terms of——

Senator DEWINE. In place, meaning that I have to fill out the information, the process is there, you know what to do with it, et cetera?

Mr. SENSER. In terms of having the foundation in place, the infrastructure, the guidance, and being able to go out to our people and educate them and say, here is the basis of our program. This is why it is important. This is what we would like you to do.

One of the lessons learned from previous implementations was that the financial disclosure program was not always well accepted and we are going to try to, again, build on that in order to ensure that the people understand the reasons behind this, what we are going to do with the information, how we are going to safeguard it, and that all those protections are in place before we begin.

Senator DEWINE. So I guess I take it from your answer—I am not trying to be argumentative here, but I take it from your answer that it is really not going to be up and running in 6 months. I mean, you are going to be moving down the road, but——

Mr. SENSER. The plan is to begin implementation in 6 months. Whether we have a fully capable program or not, I would say no.

Senator DEWINE. Well, we look forward to working with you on this and all the other recommendations. It is obviously going to be an ongoing problem and it does come back to money. It comes back to implementation and how well you all do in your management, of course, but it also comes back to the money. I think the more information that you can supply this Congress, the better off the country is going to be on that. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

I want to wrap this up, but the question that occurs for me, and for Mr. Szady, when the FBI agent Earl Pitts was caught and convicted in 1997, he had been spying for Russia, he was debriefed. He was asked about some other spies and he stated he did not know for certain, but he did mention Robert Hanssen, who had hacked into an FBI computer, and the report that we have seen says the FBI did not followup on that information. Why not?

Mr. SZADY. You sort of summarized all the abberations a little while ago with Hanssen. This was one of them. When he was interviewed, he did say—he did not say that Hanssen was a spy or anything along those lines, but he did allude to the fact that Hanssen had hacked into a superior's computer. The reason it was not followed up on is because everybody was fully aware of that. We knew

it had happened. It had happened in the past. We thought the explanation at that time was viable and we were willing to let it go at that. At the same time——

Chairman LEAHY. It did not ring a bell, why was Pitts aware of this? I mean——

Mr. SZADY. Well, there were——

Chairman LEAHY. And Pitts is a Russian spy, and the fact that he is sort of volunteering that, I mean, did everybody in the building know that Hanssen——

Mr. SZADY. Yes, pretty much. That is right, Senator.

Chairman LEAHY. They did a study afterward, a damage assessment that recommended, and I will speak generally, but it recommended looking for another Russian penetration in the FBI. That was rejected. Following Hanssen's arrest, a former FBI assistant director is quoted in the press as saying the study was right, but for the wrong reasons. The FBI and Justice Department have kept this classified, so without going into any classified details, are you satisfied that the FBI was right to reject this recommendation, particularly—well, were they right?

Mr. SZADY. Well, the investigation to find Hanssen—what we have to remember is there were investigations ongoing since the 1980's. We knew we were hemorrhaging. Even after Ames, we realized that there was somebody else. I think it was mentioned here earlier that the focus went on the CIA, but all our analytical efforts and everything at that time pointed in that direction.

We at no time, though, eliminated the FBI, which seems to be a story that is out there. We kept going back to the FBI as a possible source for this hemorrhaging. The issue was that our analytical effort, our reporting that we were getting from around the world indicated that it was more likely in the CIA, so we put our resources into that particular arena.

But at no time do we ever think there is no vulnerability for having a spy within our midst, if you will. This is an ongoing problem and always will be. Espionage is a crime. So our focus with a new espionage section is to say you just cannot rest on your laurels and you cannot say there is not a spy in any particular government agency. And hopefully, we can be preventive and proactive in the future.

Chairman LEAHY. And before everybody goes back, somebody is looking with suspicion at everybody around and feel they have got to report the person who ordered borscht at lunch and not a good American hot dog.

Mr. SZADY. Right.

Chairman LEAHY. The vast, vast, vast majority, I mean, almost everybody who has worked for the FBI and the CIA are there because, one, they are patriotic, two, they are competent, and three, they are dedicated or they would find something else to do. There are enough difficulties with the job in the first place. I think the American public has to understand that, too. It is not as though we suddenly have an FBI and a CIA riddled with spies or embezzlers or anything else. We do not. We have some extraordinarily good men and women there. You know them and I know them.

I think, though, that like in everything else, it is like the wonderful person who helps take up the collection every week at church. You still want to make sure that there are checks and balances in there, because unfortunately, sometimes there is somebody, for whatever reason, who goes bad. It is rarely ever ideological reasons, but if it is for the reasons of money or blackmail or something like that, sometimes with the right steps they can be more easily found.

We will keep the record open. I want to thank all three of you. I know you have spent an enormous amount of time on this. I know you have spent a great deal of time with my staff and Senator Hatch's staff and others in preparing for this hearing. I do very, very much appreciate it. Thank you.

[Whereupon, at 12:24 p.m., the committee was adjourned.]

[Questions and answers and submissions for the record follow.]

[Additional material is being retained in the Committee files.]

QUESTIONS AND ANSWERS

Responses of FBI Assistant Director Kenneth Senser to Senator Charles Grassley

1. *Congress has granted a huge amount of money, at least $379 million, for the Trilogy project to upgrade the FBI's computer systems and networks. Trilogy is an important project for the FBI's efficiency and information management, and I know your security people are helping. The Webster report states that even this new system is not getting enough security built in. In fact, security is an afterthought to the operations of Trilogy. I know the FBI is on a tight schedule to finish this important upgrade, but if this system is not secure enough, it's not even worth doing.*

(a) *Is security being left out as the Webster report depicts, or do you disagree and think that Trilogy has sufficient security based on your division's work on the project?*

Response: The Security Division agrees with the Commission's conclusion that Triology does not currently have the level of information systems security necessary to adequately address the vulnerabilities exposed by the Hanssen case. The original Trilogy proposal was only intended to deliver a foundational level of security protection as it up-graded the FBI's networks, workstations, and five major investigative applications. After the arrest of Hanssen, a separate information assurance initiative was developed to provide enterprise-wide "defense-in-depth". Security Division personnel are working closely with the Trilogy project and the level of security delivered will be an improvement compared to today's capabilities. Security Division will continue to focus on establishing a comprehensive, robust information assurance program.

(b) *Also, what is the FBI's priority -- finishing the upgrade on time or making sure your networks and systems are secure?*

Response: There is always potential dissonance between the quality of an implementation and its speed. A best effort is being made to meet both needs simultaneously. The FBI already delayed the Trilogy schedule once after we determined that the level of testing afforded the system would not be sufficient at the time of scheduled deployment.

When considering deployment, the Trilogy Program Manager will conduct an "Operational Readiness Review". The criteria for this review include the requirements that Trilogy be more secure than the existing network, is available for use, and includes the functional capabilities to support investigations. Trilogy will not be deployed if we cannot assure that these requirements are met.

2. *In your testimony you stated that you have the full support of and access to Director Mueller. However, if there ever comes a time where you find some unresolved security issues but you run up against some institutional opposition to fixing them, what would you do? Would you feel comfortable bringing that kind of problem to the attention of Congress? Or the Justice*

Department Inspector General?

Response: Like others working in the US Government, Mr. Senser is able to take advantage of reporting mechanisms available under "whistleblower" provisions.

3. *The Webster report recommends that the head of security report straight to the Director. I understand that your office is right down the hall from the Director's up on the 7th floor, but in terms of organization, don't you, as an Assistant Director, report through an Executive Assistant Director? Do you think that is sufficient or will the Bureau adopt the report's recommendation that the head of security report straight to the director?*

Response: The FBI established a Security Division as a means to integrate disparate elements of the Security Program and to elevate the stature of security. The division, led by an Assistant Director, has the full support and cooperation of Director Mueller. The Commission recommended that the independent security organization report directly to Director Mueller. Instead, Director Mueller decided that the Security Division will report administratively to the Executive Assistant Director for Administration. This decision was made to ensure that the Security Division will receive the level of support it requires as it relates to administrative matters (space, personnel, information systems, finance) since the Director cannot devote the time necessary to address matters of this nature for a division of this size (over 400 Headquarters positions projected by fiscal year 2003). Director Mueller still maintains the immediate oversight of security matters relating to policy and operations. The Director will write the performance appraisal of the Assistant Director with input from the Executive Assistant Director for Administration. The Director will meet with the Assistant Director whenever it is necessary to address a security matter and on a periodic basis to review division operations.

4. *In your written testimony, you indicate that the FBI intends to develop a professional security officer cadre over time. Please answer the following questions:*

(a) *How many professional security officers will the FBI hire in 2002?*

Response: The fiscal year 2002 congressional budget authorized 18 new positions within the Security Division and the 2002 Counterterrorism Supplemental authorized 36 additional positions for the Information Assurance Program. We intend to fill all 54 positions in fiscal year 2002. In addition to the budgeted positions, approximately 40 other security professionals will be hired to fill positions identified by Director Mueller as critical to the Security Program. The funded staffing level for these positions is being identified through the FBI's internal reorganization exercise which is currently underway.

(b) *How many such officers will be hired over the next three years, and at what cost?*

Response: By the end of fiscal year 2006, the Security Division will develop a comprehensive Program, consisting of approximately 900 personnel, both professional Security Officers and those supporting the Program, at Headquarters and in the field, representing 28,000 employees and thousands of contractors at more than 700 FBI locations worldwide. These employees will provide expertise in the various security disciplines, to include: (i) personnel, (ii) physical, (iii) procedural/operational, (iv) technical, (v) information assurance, (vi) education and training, (vii) force protection, (viii) construction, (ix) industrial/acquisition, (x) SCI program, and (xi) compliance. If the personnel resources included within the fiscal year 2003 request are approved, the Security Division estimates that another 350 to 400 employees will be required during fiscal years 2004, 2005, and 2006. The additional personnel costs over this same time frame will be $30 to $35 million.

(c) *Please describe your plans to adopt a career-enhancing training program for FBI security staff, as the Commission report recommends (at page 33), and tell us what resources are needed for this purpose.*

Response: It is necessary to establish the framework for the entire Security Career Service since none currently exists at the FBI. This will entail the identification of the requisite career tracks, expertice levels (e.g., entry, developmental, full performance, expert), performance rating criteria, and training requirements. The Security Division will create an education, training, and awareness staff. In conjunction with the professionals assigned to the Training Division, this staff will develop a "Security Knowledge Requirements Matrix" to identify the key knowledge, skills, and abilities necessary at each level of expertice found in the security career tracks. Training opportunities, both mandatory and optional, will be identified in the matrix.

To execute the training program for the FBI security staff, it will take 16 people and $22.2 million between fiscal years 2003 and 2006. A portion of these resources can be taken from funds included in the fiscal year 2002 CT Supplemental and those already requested in the fiscal year 2003 budget submission for general and information assurance-related security education, awareness and training.

(d) *What level of resources are needed to transform the entire FBI security program?*

Response: Between fiscal years 2002 and 2006, it will take an investment of an additional 609 to 659 positions and $388 to $443 million.

5. *The Webster Commission report indicates that "[s]ome of the weakest links in security have resulted from unwritten policies and from implementation of security policies without input from security program managers" (at page 5). How will the Bureau ensure that security program managers have input into Bureau decision-making?*

Response: Mr. Senser is in the process of realigning the FBI Security Council to also serve as the FBI Security Policy Board. This entity will serve as a mechanism for vetting all security policy prior to approval by Director Mueller. No security policy will be approved unless it has been reviewed by Mr. Senser and the Board. Security program managers will have input as the policies are developed.

6. *The Commission's report (at page 76) indicates that "FBI uniformed security police, who provide the primary line of defense against unauthorized entry at Headquarters and other facilities are understaffed, insufficiently trained, and ill equipped to deter improper removal of classified material." Please explain whether the FBI needs additional funding to upgrade its uniformed police force, and if so, how much funding.*

Response: Additional staffing and funding are required to improve police operations. Ninety additional police officer positions will be requested in fiscal year 2004 for police detachments operating at Headquarters; Quantico; Clarksburg, WV; and the Washington and New York City Field Offices. During fiscal years 2005 and 2006, assessments will be made as to whether police force operations should expand to other FBI locations or whether continuing the guard service contracts currently in place is more effective and efficient.

Additional funding will be required to conduct initial basic and recurring in-service police training; provide essential equipment to operate, such as, uniforms, vehicles, and weapons; and recapitalize aging and malfunctioning radio systems. There are no enhanced resources in the fiscal year 2003 request for police operations. Between fiscal years 2004 and 2006, we estimate a requirement of $6.2 million.

7. Robert Hanssen physically carried large numbers of classified documents out of FBI buildings. In the wake of the Hanssen debacle, what changes, if any, have been made with respect to FBI policies for removal of classified material from FBI buildings?

Response: Policies prohibiting the unauthorized removal of classified material from FBI facilities were in effect during the time frame Hanssen committed espionage and continue to be in effect today. The Security Division envisions the establishment of various programs to improve future enforcement of these policies. The programs include the conduct of random bag and package searches of persons leaving FBI facilities; the use of technology to "tag" classified materials, computer media, and documents so that their unauthorized removal would be alerting to employees stationed at the exits to FBI facilities; and, when feasible, the increased "lock down" of computer drives so that the unauthorized downloading of classified material in an electronic format will be much more difficult. Robust security education and awareness efforts will be instituted to remind the FBI population of their obligations to safequard classified material. Resource requirements for initiation of these enhanced compliance efforts will be submitted within budget requests for fiscal years 2004, 2005, and 2006.

SUBMISSIONS FOR THE RECORD

Statement of
The Honorable Orrin Hatch
United States Senator
Utah

April 9, 2002

PRINTABLE VERSION

Over the course of the last year, we have become acutely aware of the damage that FBI Special Agent Robert Hanssen has done to our national security. Over 22 years, beginning in 1979 and continuing until his arrest in 2001, we are told that Hanssen gave the Soviet Union and Russia substantial amounts of vital information affecting U.S. security.

When Mr. Hanssen's activities were discovered, we all questioned whether his ability to jeopardize our nation's security was due to deficiencies in the FBI's internal security.

Commendably, Attorney General John Ashcroft and then-Director Louis Freeh responded quickly to the crisis by appointing Judge William Webster to lead a thorough and independent review of the FBI's internal security programs.

The Webster Commission has now completed this task, and it is apparent from its extensive, well-written Report that the Commission was meticulous in its investigation. The Webster Commission's comprehensive study will guide the FBI well as it undertakes the critical task of transforming its internal security programs. I commend Judge Webster, his Commissioners, and their staff for their diligent work in compiling this Report. I want to acknowledge, in particular, George Ellard, who was Senator Biden's chief counsel on this Committee for his service as General Counsel of the Commission. Our nation owes a debt of gratitude to Judge Webster and the members of his able team for their dedication to this important review.

Reforming a multi-faceted institution like the FBI is no easy task. As the Webster Report points out, an inherent tension exists between the Bureau's law enforcement function, which is grounded in shared information, and its intelligence function, which by necessity must be grounded in some degree of secrecy. Conflicts between operational and security objectives are common. The recommendations contained in the Webster Report appear to strike a workable balance between these occasionally competing objectives, by advocating reforms that will increase the Bureau's security without jeopardizing its efficiency in the law enforcement arena.

I am pleased to hear that under the leadership of Director Mueller, and immediately before him, Director Freeh, the FBI has examined its security programs and has already incorporated many of the security reforms the Webster

Commission has recommended.

Most significantly, the FBI has established an independent Security Division, led by an Assistant Director whose role is to plan and implement the FBI's security programs. As the Webster Commission suggested, consolidating the FBI's security functions into a central office will not only increase the Bureau's focus on security matters, it will also ensure greater security coordination within the FBI.

In addition, the FBI has improved the security of its information systems, instituted frequent polygraph examinations and access reviews, and developed a comprehensive security education, awareness and training program.

We look forward to the FBI continuing to incorporate all of the reforms recommended by the Webster Commission, as the Bureau has indicated it will.

I want to take a moment to commend Director Mueller and his team. Director Mueller has been on the job for only 7 months, and during virtually his entire tenure, he has been coordinating the FBI's response to the September 11th attacks. I am sure that I am not alone in my admiration for the institutional reforms Director Mueller has already managed to accomplish under these trying circumstances. I believe as a newly installed Director, Mr. Mueller should be allowed to implement his reforms - and as I know he is aware, to be accountable for the results.

As I have said on countless other occasions, the FBI is the one of the finest law enforcement agencies in the world. We have learned, however, we cannot let our respect for the FBI as an institution, or for the many hard-working agents who are often asked to put their lives on the line, blind us from the fact that the FBI has, on occasion, come up short of our expectations. And that is a serious matter.

We must keep in mind, however, as the Webster Commission has noted, the FBI is not the only governmental entity that has been betrayed by one of its trusted employees. The General Accounting Office has reported that between 1982 and 1999, 80 federal government and contractor employees were convicted of espionage. That is an astounding number. As the Webster Commission observes, with the exception of the Coast Guard, since the 1930's, every U.S. agency involved in national security has been penetrated by foreign agents. In this information driven age, the FBI and all governmental entities must learn from their own mistakes and from those of one another to ensure that our nation's security is protected.

I applaud Director Mueller for the significant steps he has taken in his brief tenure to address the FBI's security shortcomings. I have the utmost confidence that he will continue to capitalize on the Webster Commission's study to improve the Bureau's security programs. In the months ahead, I look forward to hearing more about the FBI's progress, and I am convinced that under the able leadership of Director Mueller, the FBI will remain the world's standard in law enforcement.

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

STATEMENT OF SENATOR PATRICK LEAHY,
CHAIRMAN, SENATE JUDICIARY COMMITTEE
FBI REFORM SERIES
HEARING ON
"FBI REFORM IN THE 21ST CENTURY:
LESSONS FROM THE HANSSEN ESPIONAGE CASE"
April 9, 2002

Introduction. Since last summer, the Senate Judiciary Committee has been holding regular oversight hearings on the future of the FBI as it prepares for the challenges of the 21st Century. Today's hearing is a stark reminder that some of the challenges facing the FBI are as old as the Republic. Today, we focus on the role of the FBI as a protector of the highly classified secrets that are the crown jewels of our national security. The report by the Commission chaired by Judge William Webster, unfortunately, demonstrates the vulnerability of the FBI in fulfilling this basic function. With the American people depending more than ever on the FBI to protect it against terrorism, that vulnerability must end.

It is this Committee's responsibility to ensure that the FBI becomes is as great as it can be, and this series of FBI oversight hearings is an important part of the process, as is the legislation that Senator Grassley and I have introduced to implement many of the FBI reforms recommended by the Webster Commission.

The Webster Commission Report. The treason of former FBI Supervisory Special Agent Robert Hanssen was a shocking revelation not only to all Americans, but also to the thousands of dedicated FBI agents and personnel who work around-the-clock and in far-flung places around the globe to make this country a safer place to live and raise our families. Attorney General Ashcroft was right to ask Judge Webster and other outside experts to evaluate the FBI's security programs in light of the Hanssen espionage case. In their report, released last week, the Commission members brought to bear their collective decades of public service at the highest ranks of our government.

An extraordinarily qualified group was assembled to study these issues of national security, law enforcement and intelligence, and its report is as thorough as it is chilling. The findings are not academic. They have important implications for the FBI's operations in the post-September 11 era.

At least one of the "significant deficiencies" and "security risk[s]" documented in the Webster

senator_leahy@leahy.senate.gov
http://www.senate.gov/~leahy/

Commission's Report are the result of new policies adopted in response to the September 11 attacks and without proper consultation with security experts.

The Commission's findings and recommendations are crucial to the FBI's efforts to fight terrorism and protect national security, as will be the recommendations of the skillful Justice Department Inspector General, who is investigating other aspects of the Hanssen matter for a report he will issue later this year.

The Webster Commission's Findings. This report is another wake up call to the FBI. Yet every time a wake up call comes, the FBI's institutional reflex has been to hit the snooze button. That must change. In this oversight series of hearings, begun last year, this committee is determined to help the FBI break that pattern. Working with the Attorney General, the Director of the FBI, and others, this committee wants to help them ensure that the FBI learns from its mistakes and becomes all that the nation needs it to be. The Webster report exposes within the FBI what the report calls a "pervasive inattention to security, which has been at best a low priority in recent years."

The report describes an FBI where computers so poorly protect sensitive material that the FBI's own agents refuse to put important information on the FBI's official system. It tells the story of an FBI where background investigations for those who supposedly protect our nation's most sensitive secrets are conducted using a "checklist approach," rather than analysis.

It paints a picture of an FBI where employees are not adequately trained on basic document security practices and where there is little or no centralized analysis of security breaches. In short, the Webster Commission found not one or two problems, but "serious deficiencies in most security programs [it] analyzed within the Bureau," and that, "when compared with best practices within the Intelligence Community, FBI security programs fall far short." The report described an FBI security system that is essentially bankrupt. There are three key findings from the report that warrant our closest scrutiny.

First, the Commission found that Robert Hanssen's activities merely brought to light broader and more systemic security problems at the FBI. For instance, Hanssen's ability to mine the FBI's computer system for national secrets for more than 20 years points to serious weaknesses in information security. Hanssen himself said that "any clerk in the Bureau" could have done what he did, and he described the FBI's efforts at computer security as "criminal negligence." Hanssen's promotion to sensitive FBI positions where he was trusted with our most sensitive national secrets – all while he was a paid Soviet spy – exposes systemic problems in the FBI's personnel security processes.

Hanssen's ability to copy highly sensitive FBI documents and, as he put it, simply "bring documents out of FBI headquarters without ... ever having a risk of being searched, or looked at, or even concerned about," reveals serious shortcomings in both document and physical security at the FBI which must be addressed. In short, Hanssen, cunning though he may be, was able

simply and easily to take advantage of the FBI's systemic security defects. Those defects must be fixed.

Second, the Commission found that the best way to protect information is not to shut down information flow completely either within the FBI or from the FBI to outsiders. Indeed, that type of reaction is inimical both to a free society and to effective law enforcement. Instead, the Webster Commission found that the FBI needs to do a better job of what is known as "defense-in-depth" security – that is, identifying what is truly sensitive information, and then creating a layered approach to protect it. Most critically, that means enforcing all important "need to know" rules, which are largely ignored at the FBI, and doing better security training of FBI employees.

Finally, and most disturbing, the Commission found that the systemic problems which allowed Robert Hanssen to compromise national security for so long are not ancient history, but they permeate today's FBI. Most alarming to me, the Commission found that decisions since September 11 have resulted in "substantial sensitive source material" from FISA surveillance being made generally accessible on the FBI's computers to FBI personnel and then being inadequately protected.

The Commission points out this breach not only presents a security risk which must be corrected "as soon as possible," but it is a breach that also could create constitutional issues which might endanger terrorism prosecutions. This was all done without consulting Justice Department officials or security experts. The report is clear: When the post-September 11 crunch was on to investigate at all costs, security was once again discarded at the risk of jeopardizing sources and methods that are critical to gathering intelligence on terrorism and to other national security interests. Who will agree to become a confidential source for the FBI, or for other agencies that share sensitive intelligence with the FBI, if effective safeguards are not in place to prevent disclosure to another Hanssen?

I must also add that, as one who helped write the USA PATRIOT Act -- which gave the FBI new surveillance powers-- and as one of many who is dedicated to proper congressional oversight of the proper use of that new power until its sunset, the Webster Commission Report raises particular concern. As the report makes clear, the FBI's actions since September 11 "send[] a clear message that the FBI's security organization is irrelevant during an operational crisis." In addition, the report raises concerns that security features in Trilogy, the FBI's billion-dollar computer upgrade, are also being sacrificed in return for short-term operational benefits.

The Commission acknowledges the basic tension between conducting effective law enforcement, which often requires information sharing, and protecting intelligence operations, which often requires restricting the flow of information to prevent compromising valuable sources. The Commissioners pointedly state that "whether the two can co-exist in one organization is a difficult question . . . ." That tension has been especially acute since September 11, but the FBI, facing pressing investigative needs, cannot continue to sacrifice long term interests in preventing future national security threats for the sake of investigating crimes that have already occurred.

The Report's Recommendations. The FBI should respond to the alarms set off by this report not by denying the problems, but by confronting them and rebuilding its security from the ground up. The Hanssen case proves that circling the wagons does not work when the enemy is already inside the circle. Director Mueller has already begun taking some important steps in the right direction, but he needs to do far more, and I will continue to support him in that effort. The Commission makes some important recommendations for improvement, and I am confident that Director Mueller will conscientiously consider them. Of the many fine recommendations, one common sense proposal stands out: to establish a system under which security lapses in any one particular agency can lead to improvements throughout the entire intelligence community.

That way, as the Commission points out, our country can establish a coherent nationwide approach to security. The Commission specifically cites a proposal for such National Security Program that I made sixteen years ago, when I was Vice Chairman of the Intelligence Committee and Judge Webster was FBI Director. The Intelligence Committee issued a report in 1986 on "Meeting the Espionage Challenge" after we had gone through the horrendous "year of the spy" with Walker, Whitworth, Howard, Pollard, Chin, and other spies detected in highly sensitive U.S. military and intelligence organizations.

Today, a national response is equally essential given the continued pattern of espionage cases last year that included not only Hanssen, but also the top Cuban analyst in the Defense Intelligence Agency who was caught spying *for* Cuba throughout her entire 15-year career, and the alleged attempt by a retired military officer working as a contractor in the National Reconnaissance Office to sell intelligence secrets to the highest bidder. The best example of why the Commission's message must go beyond the FBI is financial disclosure. The report concludes that the FBI failed to examine Hanssen's finances, partly because of a poor security re-investigation and partly because the FBI did not implement an Executive Order requirement for regular financial disclosure by employees in the most sensitive positions. In this failing, the FBI is not alone.

Most departments and agencies, other than the CIA, did not implement this requirement when it was adopted after the Ames case, based on a 1994 Congressional mandate in section 801 of the National Security Act, and nothing more has been done since Hanssen's arrest over a year ago. Hanssen told the Commission, "The only thing that possibly could have uncovered my espionage activities was a complete investigation of my financial positions and deposits to bank accounts."

I call on the Administration to act immediately to ensure that all relevant departments and agencies implement the financial disclosure requirement in current law. Security against espionage is a national challenge that should not be left to each individual agency without accountability.

The Need for Congressional Action. Too often in the past, recommendations and reports like these have not been treated as real opportunities for reform but as occasions to roll out the spin machine. In fact, on the security issue, the 1997 Justice Department Inspector General's report

on the Aldrich Ames spy case specifically warned that the FBI needed to "develop and maintain a better record-keeping system for tracking" top secret documents, some of the very things which Mr. Hanssen later stole.

I cannot help but think that, as then-FBI Agent and Russian spy Hanssen read the I.G. report, he knew that he could go on just as before, and that the report would wind up in some FBI filing cabinet, never to see the light of day. That cannot happen yet again. That is why Senator Grassley and I have introduced S.1974, the FBI Reform Act of 2002. Our bill calls for many of the reforms now echoed in the Webster Commission Report.

> **(1) Career Security Program**. The report calls for an FBI career security program with status equal to Special Agents. S. 1974 establishes this program to strengthen skills, training, status and leadership for FBI security personnel.
>
> (2) **Employee Screening Polygraph Authority.** The report endorses regular counterintelligence screening polygraphs for FBI personnel in the most sensitive positions. S. 1974 authorizes such a program with safeguards against misuse.
>
> (3) **FBI Computer Security**. The report says FBI should make progress reports to the oversight committees for three years. S. 1974 requires a report on FBI computer security and access controls for classified and sensitive but unclassified information.
>
> (4) **FBI Police Authority**. The report recommends improving the FBI security police force. S. 1974 authorizes better pay and benefits for FBI police who guard FBI facilities.
>
> (5) **FBI Counterintelligence Authority.**. The report stresses the importance of the FBI's counterintelligence role. S. 1974 requires a report from the Attorney General on the FBI's legal authorities, including the need for legislation to replace current non-statutory authority for FBI counterintelligence functions.
>
> (6) **FBI Security Whistleblowers.** The Commissioners found that "few FBI security violations are reported to security" and, even if reported, violations are not tracked. The Commission proposes a Security Incident Reporting Program to ensure proper reporting and investigation of security violations. Security violation reports will remain few unless personnel doing the reporting feel protected doing so. S. 1974 provides safeguards for FBI whistleblowers who complain when superiors do not remedy security problems.
>
> (7) **Inspector General**. The entire report shows the need for independent, outside review of FBI problems in security and other fields. S. 1974 codifies the authority of the Justice Department Inspector General to conduct such reviews.

At a hearing with the FBI and the DOJ Inspector General several weeks ago on the belated production of documents in the Oklahoma City bombing case, witnesses before our committee

supported codifying the Inspector General's authority to investigate the FBI, enhancing FBI whistleblower protection, ending the double standard whereby senior FBI management are disciplined less severely than rank and file agents, and coming up with a 10-point plan to move the FBI's computer systems into the 21st Century. The need for legislation to help reform the FBI is real.

The days of hands-off oversight of the FBI are over, and these hearings serve as a catalyst for reform by encouraging the FBI, under Director Mueller's leadership, to continue its needed improvements. That is why we are holding, and will continue to hold, these bipartisan FBI oversight hearings.

Now, more than ever, the nation needs the FBI to live up to its potential. In combating terrorism on our shores, the FBI needs to be stronger and smarter and more effective than ever. The stakes are too great and the price too high for anything less.

# # # # #

Statement for the Record

Kenneth H. Senser
Assistant Director, Security Division
Federal Bureau of Investigation

before the

United States Senate
Committee on the Judiciary
Washington, D.C.

April 9, 2002

Good morning Chairman Leahy, Senator Hatch and other members of the Committee. I spoke to you initially on July 18, 2001, about our analysis of the FBI Security Program and the work we are doing to transform our internal security operation into one fully capable of addressing the diverse and formidable threats facing the Bureau. I am very pleased to be back again to provide the Committee with an up-date regarding the FBI's progress on this matter and to commend the comprehensive and extraordinarily helpful work performed by Judge Webster and his Commission on the Review of FBI Security Programs.

Your continued interest in ensuring that the FBI operates in a secure environment is much appreciated because without the support of Congress, this badly needed transformation would not be possible to complete. We also commend Judge Webster and his Commission for the extremely detailed and independent review of the FBI's internal security program. The product of their efforts will serve the FBI well as a measuring stick on where we need to be on the multiple fronts that affect our internal security. When then Director Freeh and Attorney General Ashcroft asked Judge Webster to undertake this critical task, our hope and expectation was exactly as he and the Commission delivered, i.e., a comprehensive and brutally candid assessment of where we are and where we need to be. It will be our roadmap.

As I mentioned in previous testimony, prior to the arrest of former Special Agent Robert P. Hanssen for espionage, the FBI had taken some limited steps to improve its Security Program, a program that was fragmented, dispersed across several different divisions and substantially inadequate in a number of respects. The Program lacked an integrated vision and security initiatives were often poorly coordinated, inefficient, and not effective. Succinctly put, security, other than physical security, was not inculcated into the culture as a priority that must be practiced, observed and improved upon everyday. Additionally, as I testified previously, the FBI identified in early 2000 seven areas within the Security Program requiring greater focus. Through his recommendations, Judge Webster provides specific and sound guidance on each area.

Since my July testimony, two other United States citizens have been arrested for espionage -- Brian P. Regan, a former member of the Air Force assigned to the National Reconnaissance Office, and Ana Belen Montes, an employee of the Defense Intelligence Agency. Additionally, on September 11th, members of Al Qaeda conducted a heinous act of terrorism against the United States. These actions validate the premise that there are adversaries of the United States that will stop at nothing to harm the interests of this country. The FBI, our many employees and the sensitive information in our files are attractive targets for a wide variety of opponents who continuously strive to impede investigative operations, obtain that sensitive information, and initiate and implement reprisal actions against Bureau personnel or facilities. For all of these reasons, I will confine my public remarks to a more generic description of the progress made by the FBI and I would be pleased to provide the Committee with a more comprehensive briefing in a closed session.

Webster Commission Recommendations

Judge Webster identified the need for extensive improvement throughout the FBI's internal Security Program. His report concludes that there are serious deficiencies in most security elements analyzed in the course of the study. Some of the identified vulnerabilities are more critical than others and represent a more significant level of risk to the security of FBI operations. The Commission grouped its recommendations into the following categories:

- Organizational Structure
- Information Systems Security
- Personnel Security
- Document Security

A review of the vulnerabilities serving as the basis for the Commission's recommendations provides traceability to the original seven critical areas previously identified by the FBI as badly in need of improvement. While of little consolation, the Commission found no others. That does not, however, mitigate the severity of the shortcoming that had developed over the years or the urgency that must attach to fixing these problems. With that we are in total agreement with Judge Webster.

Since Hanssen's arrest in February 2001, the FBI has been engaged in a dedicated effort to transform its Security Program and we very much appreciate the help and guidance of Judge Webster's staff regarding these efforts. The severity of the shortcomings and corresponding vulnerabilities dictated that we proceed even while this outside review was ongoing. Because of their help, the two efforts were complimentary, which allowed much progress to be made. As Judge Webster points out, much more progress is still required. The Webster Commission report and recommendations will be an extremely valuable tool in this process.

The remainder of this statement will be devoted to bringing the Committee up-to-date on what has already been accomplished and a brief description of the additional Security Program improvements we plan on making in the future, guided, of course, by the recommendations and observations reflected in the report.

Status of the Interim Security Improvements

In late March 2001, former Director Louis J. Freeh took a number of internal security-related actions designed to immediately improve the internal security of the FBI. These steps included the appointment of a task force of Assistant Directors (ADs) to ensure the complete identification and effective implementation of the interim security improvements, the removal of the Security Program from the National Security Division (NSD) and its establishment as a stand-alone entity reporting to then Deputy Director Thomas J. Pickard, my appointment as the executive manager responsible for the direction of the Security Program, and the adoption of a detailed security policy process.

The following additional interim security changes were initiated:

Enhanced Computer Audit Procedures: The Webster Commission report describes how Robert Hanssen easily compromised the information contained on approximately 26 computer diskettes, representing about 6000 pages of material, much of it obtained through his exploitation of a critical FBI investigative database, the Automated Case Support (ACS) system. Hanssen did not need to "hack" inside the computer system. His "legitimate" permissions allowed him to surf the system and find information of value to support his continuing espionage.

Shortly after Hanssen's arrest, former Director Freeh instructed our personnel to implement regular reviews on our most sensitive cases -- reviews that can highlight all individuals who have looked at the case files -- so that the case agents and their supervisors can be responsible for assuring these cases are being accessed by only those with a need to know. A process was established, using the regular file review mechanism whereby agents discuss investigative progress with their supervisors every 90 days, to review the Document Access Report within the Electronic Case File segment of ACS. Through this review, case agents assigned to the most sensitive investigations are responsible for resolving potential unexplained accesses.

Initiation of this process is an excellent start, but remains inadequate. One major shortcoming of ACS is the complexity of its operation and the lack of user friendliness. The Webster Commission report highlights that while ACS contained these case audit and tracking tools from its inception, few users knew they were available or did not understand how to access them. Ultimately, this vulnerability will be mitigated through the implementation of a new case management system called the Virtual Case File (VCF) and the application of robust Information Assurance (IA) principles which will be described in greater detail below. Both of these were discussed at a recent hearing before this Committee. With the funding Congress has provided,

the FBI will make a giant leap forward on both managing information and managing the security of information.

To address this issue until the VCF and IA Program is viable, the FBI's Information Resources Division developed a user friendly application called the Case Document Access Report (CDAR) which will facilitate the case auditing process and provide the case agent and his or her supervisor more oversight capabilities. The CDAR has just finished the certification and accreditation process, required of all new software applications, and deployment will begin soon. In conjunction with this deployment, more focused education and awareness will be provided to ACS users on the security associated with the ACS investigative database.

Expanded Polygraph Program: During the course of Hanssen's Bureau career, he never took a polygraph examination. In 1994, the FBI established a requirement to test all new employees prior to them beginning their service. Additionally, individuals with access to certain sensitive programs or cases were polygraphed and it was also used during serious internal inquiries to resolve unexplained anomalies and ambiguities.

Former Director Freeh ordered after Hanssen's arrest periodic polygraph examinations for those individuals, who by the nature of their assignment, have broad access to our most sensitive information. Polygraph examinations were also ordered for those employees serving in overseas assignments.

Since the limited polygraph expansion became effective, close to 700 counterintelligence (CI) -focused examinations have been conducted. While the initial population of employees occupying positions with access to the most sensitive information was estimated to be close to 550, this population is dynamic. For example, as employees have retired, new incumbents for these positions were chosen and, ultimately, polygraphed. The vast majority of employees who were polygraphed have successfully completed the process. We are continuing to work with slightly more than one percent of the tested population to resolve anomalies. We developed a process for attempting to resolve anomalous outcomes which takes into account the fact that polygraph is only one element of a healthy personnel security vetting program and assures that, while it may be necessary to modify the sensitivity of an employee's access to information during the inquiry, no adverse action will be taken against the employee based on polygraph results alone. While no admissions have been surfaced during the polygraph examinations to date that are of a seriousness equivalent to that of the Hanssen case, the process has identified lesser security transgressions and other behavior that has resulted in referrals to the FBI's Office of Professional Responsibility (OPR) for appropriate disciplinary considerations. This is a necessary component of changing to a culture of security awareness.

FBI Director Robert S. Mueller, III, recently agreed to a new risk-based framework for the Polygraph Program and slightly expanded the pool of employees subject to CI-focused examinations. I will discuss this in greater detail later in my statement.

Enhanced Reinvestigation Analysis: The Webster Commission report identified a number of issues that surfaced during Hanssen's 1996 security reinvestigation that should have been recognized as "red flags." Statements were made by some references that did not appear to have been pursued by investigators and there was no indication that security clearance adjudication personnel did much more than complete a "check list" when deciding to favorably rule on the case. There were other questionable incidents during Hanssen's career that were never integrated into a rigorous analytical process which could have resulted in a decision to further scrutinize his trustworthiness.

Former Director Freeh mandated in March 2001 that an enhanced analysis capability within the Security Program be established to conduct security adjudications and to resolve any anomalies resulting from the reinvestigations of persons with access to the most sensitive information. We established a separate unit within the Security Program for this purpose. The unit also serves as the point for CI-security integration. It is staffed by an agent Unit Chief and two agent supervisors. Fourteen contractors (retired FBI agents) are conducting analysis. Additional staff resources have been allocated to establish an enhanced financial analysis capability. Their mission is simple: ensure that pieces of information that are potential "red flags," regardless of how disparate they may be, get fully analyzed, investigated and resolved in an expeditious fashion. That did not happen in the past.

As with the expanded use of polygraph, we have identified some security transgressions via the enhanced analysis process and other behavior that has resulted in referrals to the OPR. Additionally, in at least one instance, this new unit identified poor operational practices that could have negatively impacted our ability to conduct effective CI investigations. As a result of this discovery, remedial actions were taken. Again, these referrals, while addressing individual shortcomings, are an important part of changing the culture to one that accepts security and security awareness as a fundamental element of conducting the business of the day.

Other Measures Implemented: During my testimony in July 2001, I described a number of other initiatives directed by former Director Freeh to facilitate the continued incorporation of security into the FBI culture so that it is recognized as an integral part of operations. These initiatives included:

- Elevating the role of the Security Officer in the field by requiring that they have a direct reporting capability to the Assistant Directors in Charge or Special Agents in Charge.
- Requiring that each Assistant Director in Charge or Special Agent in Charge establish a Security Council.
- Developing and conducting training for FBI employees and, in relation to job-specific requirements, Security Officers.
- Receiving security expertise and support from the Intelligence Community.
- Improving the security of Sensitive Compartmented Information (SCI).

Significant additional progress was made in these areas as well as others since July. This progress will be further developed later in my statement.

Status of the Transformation of the FBI Security Program

I previously described to the Committee the fragmentation and disarray of the FBI Security Program which were captured in the seven critical focus areas. The Webster Commission report clearly illuminates the degree to which security was "broken". If there was ever any question, it should now be obvious that what is required is not a "band aid" approach, but a complete transformation of the Security Program. During the July testimony, the Committee learned about a prioritized list of 15 initiatives that would serve as the roadmap for the transformation. I indicated that while the categories were prioritized, it would not be effective to cut the proposal into pieces. I also stressed that a transformation of this magnitude will take time. It must be carefully planned and executed and it must be inculcated into our employees.

So as to give the Committee a better perspective of the full range of security improvements initiated during the last year, our accomplishments are arrayed, along with some of those efforts we plan on completing in the future, against the groupings used by the Webster Commission.

Organizational Structure: Prior to Hanssen's arrest, there was no integrated FBI security architecture or structure. Elements of the Security Program were disseminated within eight different organizational components. This fostered an organizational disregard for security and a culture at the FBI that did not react to symptoms of Hanssen's activities. In response to this, since July 2001, the FBI:

- Established a Security Division which, for the first time in FBI history, will serve as a point of integration for all Bureau security matters.
  - Moved the programmatic responsibility for facility protection and police services to Security Division, as well as the operational responsibility for protecting FBI headquarters and the Washington Field Office.
  - Moved the Polygraph Unit to the Security Division.
  - Started the development of a joint "business plan" with the Laboratory Division to ensure technical security resources are properly directed against Security Division requirements.

- Appointed a Director of Security, at the Assistant Director level, who serves as the senior security executive. This AD has the full support of and direct access to Director Mueller who has strongly communicated his support for the Security Program to all FBI employees.

- Provided needed infrastructure support to the Security Program by:
  - Shifting internal resources to the Security Division as part of the on-going FBI restructuring plan.
  - Establishing additional "detail" assignments to the Security Division from the Central Intelligence Agency (CIA) and the National Security Agency (NSA).
  - Applying resources received in the fiscal year 2002 budget process to security requirements.
  - Submitting a fiscal year 2003 budget request that includes significant resources for the Security Division and its mission.

- Initiated a comprehensive review of national, Director of Central Intelligence, Department of Justice, and FBI policy directives to establish a traceability matrix that will be used to gauge the effectiveness of existing security policy.

- Initiated the development of a comprehensive security education, awareness, and training program. The initial objective of this program will be to address information systems security issues followed by an expansion to all other elements of the Security Program.

Some of the initiatives the FBI intends to accomplish in the future include:

- Evaluating the need for and developing resource requests to mitigate security vulnerabilities to a level where the risk is acceptable.

- Seeking to further consolidate security functions within the Security Division.

- Developing a professional Security Officer cadre through the establishment of a comprehensive career program that identifies and hires candidates with appropriate skills, successfully retains them via a competitive pay and reward structure, builds expertise through appropriate training and assignment opportunities, and prepares them to assume program and management roles of increasing responsibility. Elements of this initiative will include:
  - Establishment of a Security Career Service Board that focuses executive attention on all elements of the professional Security Officer career track.
  - Certification of proficiency for security professionals and key non-security personnel, such as system administrators, in critical job-related skills.

- Re-designing the field Security Officer program to:
  - Rely less on agents and more on the professional Security Officer cadre we intend to build over time.
  - Restructure the field offices so that all security responsibilities fall under the control of the Security Officer.
  - Direct more resources to the field to support the Security Program.

- Modifying the operation of the FBI Security Council to ensure it is appropriately staffed by senior executives and addresses security policy issues of significance to the Bureau.

Information Systems Security: Under the earlier section addressing the interim measures taken to enhance the computer audit procedures, I described how Hanssen exploited ACS to compromise FBI information. Protection of information within Bureau information systems is a particularly critical issue. Of the 15 initiatives that comprise the FBI's security roadmap, six directly relate to information systems security or information assurance (IA).

The Webster Commission report accurately points out that the FBI's information technology (IT) recapitalization effort, Trilogy, includes funding for only the foundational elements of IA. At rollout, Trilogy will provide more security than the FBI's current IT backbone and the five investigative applications it addresses, to include the ACS. However, the goal is to develop the IA Program to be on par with other world-class information systems security efforts. Significant coordination has taken place between the Trilogy Program and personnel assigned to the IA Program to ensure that the Trilogy security architecture will support the utilization of the future IA technologies we plan to employ, such as public key infrastructure (PKI).

In order to address security vulnerabilities impacting FBI information systems, since July 2001, the FBI:

- Established an IA Program within the Information Resources Division.
- Developed a detailed spending plan for executing IA Program resources received as part of the FY 2002 Counterterrorism supplemental appropriations bill.
- Developed a fiscal year 2003 budget request to continue development and implementation of a robust IA Program.
- Sought and received Director Mueller's commitment to appropriately address the delinquent certification and accreditation (C&A) status of many FBI IT systems.
- Implemented an aggressive C&A effort to discover and address vulnerabilities within existing and proposed FBI IT systems.
- Collaborated with the Trilogy Program to immediately deliver enhanced security measures and to provide the framework for improved information systems security measures in the future.
- Initiated the modernization of cryptographic key management to improve the security of FBI information and to facilitate the immediate deployment of Trilogy infrastructure.

Some of the initiatives the FBI intends to accomplish in the future include:

- Assigning an experienced IA professional from the Intelligence Community (IC) to run the FBI's IA Program and adding strategic "consulting" resources from the IC, as appropriate.

- Designing a comprehensive IT security architecture for FBI systems. As part of this architecture, identifying the baseline for IA tools or techniques, such as PKI, virtual private networks and LANs, single sign-on, intrusion detection, network scanning, auditing, and other methods to identify anomalous activity and system vulnerabilities.

- Establishing an Enterprise Security Operations Center to centrally manage the security of FBI IT systems and networks.

- Re-evaluating and improving the certification and accreditation process so that it mirrors best practices and is tied to the IT system development life cycle.

- Establishing a number of experienced Information Systems Security Managers as customer focal points for expeditious handling of IT security questions and issues.

- Continuing the close collaboration between IA and Trilogy Program personnel to implement improved IT system security as part of the on-going Trilogy effort.

Personnel Security: The Webster Commission report identifies many shortfalls in the processes used to assess Hanssen's continued trustworthiness. I described some of these deficiencies earlier in my statement when discussing the interim steps we have taken to expand the Polygraph Program and to conduct enhanced reinvestigation analysis. In order to improve our Personnel Security Program, since July 2001, the FBI:

- Implemented a written case summary format for reviewing security adjudication recommendations.

- Moved Polygraph Unit from the Laboratory to the Security Division.

- Continued to conduct polygraph examinations according to the criteria established in March 2001 as part of the limited expansion.

- Received conceptual approval by Director Mueller to continue with a limited and careful expansion of the polygraph program. The formal decision memo has been generated for his signature. The proposal:
  - Expands the population already subject to CI-focused polygraph examinations to all personnel involved in the CI, CT, and Security Programs.
  - Establishes a risk-based program comprised of four elements -- for both employees and non-Bureau personnel -- with access to the most sensitive FBI information. The elements include:

- ✓ Examinations as part of initial applications for employment or access.
- ✓ Periodic examinations tied to security reinvestigations.
- ✓ Aperiodic or random examinations.
- ✓ Compelled examinations if necessary to resolve issues that impact trustworthiness as defined by Executive Order 12968 and the Adjudication Guidelines that implement it.

Some of the initiatives the FBI will accomplish in the future include:

- Defining the requirements for an integrated security information management system and data integration efforts, as well as, executing a limited number of "pilot" efforts using funds received in the fiscal year 2002 appropriation.

- Working with the Records Management Division to improve control of FBI security files and ensure they contain the necessary information. Eventually, as part of the effort to develop an integrated security management system, transitioning to an electronic security file.

- Automating security data collection processes in a web-enabled environment.

- Identifying new sources of information that add value to the vetting process and assist in the determination of trustworthiness of employees.

- Establishing a broad based Financial Disclosure Program and developing the capability to conduct security-related financial analysis.

- Exploring the use of a specific-issue polygraph examination to address the concern of deliberate unauthorized disclosure of FBI information.

Document Security: The Webster Commission report depicts an environment where Hanssen was able to perpetrate his espionage with impunity. In one anecdote, the report describes how Hanssen is able to walk into an office area where he used to be assigned without being challenged and log onto a computer system to retrieve sensitive information which he ultimately compromised to the Russians. The Commission indicates that even recently, based on the personal experiences of their investigative staff, FBI employees still leave secure areas unattended at times potentially providing unfettered and unauthorized access to sensitive documents.

In order to continue improving the protection we afford to documents containing sensitive information, since July 2001, the FBI:

- Reassessed access procedures for FBI facilities eliminating special exemptions afforded executives.

- Established the position of Special Security Officer for the FBI and selected an Intelligence Community officer to serve in this role as a detailee.

- Completed a review of SCI handling procedures.

- Conducted a comprehensive review of sensitive accesses resulting in a net decrease of FBI employees with SCI.

- Conducted a "Back-to-Basics" day for all employees where security was one of the key areas of focus.

Some of the initiatives the FBI will accomplish in the future include:

- Establishing a Security Incident Reporting Program that includes management of all potential information compromises through a central, Security Division component. This component will ensure the security incidents are properly investigated; assessments are conducted of potential damage to the national security or FBI operations; remedial action is taken, as necessary, to ensure the compromise does not happen again; and personal accountability is assigned, if appropriate.

- Establishing a capability to resolve security anomalies, no matter their source, and to integrate information resulting from the investigation of these anomalies into the FBI CI Division.

- Developing an enhanced capability to securely process SCI electronically.

- Developing an appropriate accountability and tracking system for sensitive hard copy documents.

- Investigating technology to better account for and track sensitive information and the media, paper or magnetic, on which it is stored.

- Developing and conducting training on the proper classification of, accounting for, and control of classified information.

- Developing a more robust set of FBI classification guides.

Summary

We have made a great deal of progress in improving security at the FBI over the last year. This is particularly true considering the crisis faced by the FBI in responding to the September 11, 2001, terrorist attacks. Response to this unprecedented crisis taxed the entire FBI, to include

the immature security infrastructure.

In the end, however, the most important change that must take place is a dramatic adjustment in the security "culture". Continuing security education, wide-spread security awareness and making security accepted as a normal part of everyday business is a cultural hurdle that must be overcome. A number of the efforts I have already discussed are designed to effect this adjustment. These include a strong statement of support for the Security Program by Director Mueller along with tangible consequences for failing to comply with security policies; consideration of security as a critical element of all operational programs; a robust security education, awareness, and training program; and, the development of understandable, relevant, and enforceable security policies.

There also must be no mistake about the fact that we are only beginning a journey that will take significant time and the future support of this Committee along with the rest of Congress to ensure success. We will continue to carefully examine the classified annexes of the Webster Commission report so that we can benefit from their comprehensive study and strengthen our action plan. We also will review the Department of Justice Inspector General report on Hanssen, expected later this year, to evaluate their conclusions and recommendations.

The Webster Commission report recognizes that the FBI, or any agency that processes sensitive information, can never totally prevent espionage. There will be, at some point in time, another FBI employee or contractor who betrays our trust. Therefore, as Judge Webster suggests, we will strive to deter those rational persons who may be contemplating a compromise of sensitive Bureau information, minimize the time between their "defection and detection", and take whatever steps possible to minimize the resulting damage.

Mr. Chairman, I appreciate the opportunity to address this Committee and all of the support you and your colleagues have provided to the FBI so that we are able to faithfully discharge our important duty and help safeguard the interests of our great nation.

Statement for the Record

David Szady
Assistant Director, Counterintelligence Division
Federal Bureau of Investigation

before the

United States Senate
Committee on the Judiciary
Washington, D.C.

April 9, 2002

Mr. Chairman, Senator Hatch, and other members of the Committee, I would like to express my appreciation to you for inviting me to share my thoughts and provide you with an update on the changes we are making to the Counterintelligence program at the Federal Bureau of Investigation (FBI). I am pleased to be appearing jointly today with Kenneth Senser, Assistant Director of the FBI's recently established Security Division. By necessity the cooperation between our two Divisions is complementary and seamless. Our Director is committed to protecting the full range of U.S. national security interests and has made counterintelligence, along with counterterrorism and prevention, his highest priorities.

Because the world has changed so dramatically, the FBI is making significant changes to its Counterintelligence program. Our end goal is more effective and efficient detection, prevention, and disruption of hostile foreign intelligence activity directed against the United States and its interests. The FBI appreciates your support as we continue to implement these changes across our organization. First, I would like to provide a very brief assessment of the characteristics of the foreign intelligence threats of the 21st Century, for they provide a basis for understanding our new national, centrally managed counterintelligence strategy.

The Threat Environment

The United States today faces an intelligence threat that is far more complex than it has ever been historically. The threat is increasingly asymmetrical insofar as it seeks to exploit the areas where there is a perception of weakness within the U.S. national security approach and organizations. Traditional notions of counterintelligence that focus on hostile foreign intelligence services targeting classified national defense information simply do not reflect the realities of today's complex international structure. Foreign targeting of the elements of national power, including our vibrant national economic and commercial interests, continues to evolve. While traditional adversaries were limited to centrally controlled national intelligence services, today's adversaries include not only

these traditional services but also non-traditional and non-state actors who operate from decentralized organizations. Moreover, the techniques and methodologies used to target classified, sensitive, and commercially valuable proprietary information march forward with the advance of technology.

This new environment and the uncertain future that accompanies it present the FBI with new challenges. The FBI's role as the leader of the nation's counterintelligence efforts requires that we understand all dimensions of the intelligence threats facing the nation and match them with new and innovative investigative and operational strategies. The FBI must continually assess and measure its performance against ever-evolving threats found in these new and different environments. The constant parade of new technologies, the vulnerabilities created by them, the extraordinary value of commercial information and the globalization of everything are but a few examples. The FBI must focus its resources on those actors that constitute the most significant intelligence threats facing the nation, wherever that might come from and in all of these new arenas.

The FBI Response

In response to the increasingly complex intelligence threat environment, the FBI is taking measures that re-orient its counterintelligence strategy, prioritize intelligence threats, and make the requisite organizational and managerial changes to ensure U.S. national security interests are protected. The following initiatives are underway:

Nationally-Directed Strategy

We recognize that in order to mitigate the intelligence threats our country is now facing, we must continually redesign our Counterintelligence program. Historically, when the threat lines were more clearly drawn, counterintelligence at the FBI was largely decentralized, with field divisions setting local priorities and assigning resources accordingly. To effectively recognize and counter the extremely diverse intelligence threats now evolving, a new more centralized and nationally directed, focused, and prioritized program is more effective. By centralizing our program we will ensure the ability of the FBI to be more proactive and predictive in protecting the critical national assets of our country. Centralization cements accountability regarding counterintelligence program direction, control and leadership. Moreover, a centralized counterintelligence program facilitates the FBI's cooperative and collaborative interaction with other members of the United States Intelligence Community. The counterintelligence environment must be transparent.

Our National Strategy will be totally integrated with the Office of the National Counterintelligence Executive (NCIX), or CI-21, to ensure that our efforts are focused on policy driven priorities and that we are positioned to protect identified critical national assets. Our efforts will also be seamless with the CIA to ensure that our counterintelligence efforts extend worldwide.

As part of this nationally directed strategy, I have undertaken a comprehensive strategic planning effort that is providing the FBI with the framework in which to prioritize and address intelligence threats. This framework is based on community-wide analysis and direction and recognizes that there can never be unlimited resources so we must be focused on the greatest threats. This will better position the FBI for the future by changing our performance expectations, management practices and processes and workforce. The central elements of this initiative are:

- Development of clear strategic objectives and operational priorities in support of those objectives. As the Assistant Director of Counterintelligence for the FBI, I have responsibility for meeting these objectives and will be held accountable for their successful implementation. Some characteristics of this effort include the establishment of:

  - A highly trained and specialized Counterintelligence workforce with a management team that reinforces counterintelligence as a specialized priority career within the FBI.

  - A much stronger operational component within the Counterintelligence Division to include a stronger program management role and specific accountability at Headquarters.

  - An ongoing system of accountability that clearly defines responsibilities for all elements of counterintelligence both at Headquarters and in the field; and

  - An enhanced communication strategy that is more effectively communicating counterintelligence policy, plans, priorities, and management concerns throughout the counterintelligence program.

  - Greatly enhanced analytical support that relies more extensively on highly specialized disciplines and that is interwoven into the intelligence community as a whole.

Organizational Changes

Accepting responsibility to prevent and disrupt foreign intelligence threats and espionage from threatening U.S. national security requires the Counterintelligence Division to adopt a more proactive posture, the kind envisioned by CI-21. In order to fully evolve to this posture, the FBI is developing operational strategies that strategically align our resources in a manner consistent with community-wide national priorities. A fully proactive posture also requires candor in acknowledging our limitations and constraints, and courage in committing ourselves to confront and overcome them. One organizational change I have made consistent with this goal is the establishment of a Counterespionage Section within the Counterintelligence Division from existing base

resources. This new section is responsible for managing all of our major espionage investigations. The section also evaluates and prioritizes all existing espionage cases to ensure effective allocation of financial and human resources and expertise to these top priority cases. I want to ensure that these cases are being handled and managed by the most highly skilled and trained FBI personnel.

Resources

In order to meet the challenges ahead of us, I am ensuring that the most important resources the Counterintelligence Division has, its human resources, have the appropriate tools available to effectively implement our mission. While the FBI has historically provided counterintelligence training to new special agents and support personnel and provided specialized courses as advances training, a systematic approach to a comprehensive counterintelligence training regimen applicable throughout an Agent's career has not been in place. The FBI is currently studying its counterintelligence training program. Agents and analysts assigned to work counterintelligence should have a systematic and integrated training program that allows them to continually refine their operational, investigative and analytical skills as their careers advance and a program to ensure that FBI counterintelligence personnel have the same knowledge and understandings as those elsewhere in the community.

Analysis is another area of my focus. Counterintelligence analysis is central to our program, as it not only provides tactical support to ongoing investigations and operations, but is also integral to providing strategic analysis in assessing the foreign intelligence threat we face. With the dissolution of the Investigative Service Division (ISD), many of the counterintelligence analysts have returned to the Counterintelligence Division. It is my job, working with our training Academy and our new college of analytical studies, to have in place a world class analytical function that operates seamlessly within the larger community effort. I think today's challenges require much greater reliance on, and bring in much greater numbers of, outside subject matter experts to bolster our efforts and understanding.

Information management and intelligence sharing are also two areas that we are improving in concert with the directives established by Director Mueller regarding these subjects. The technology being put in place at the FBI will vastly increase our capability to maximize the value of what we know and, even more basic, to know what we know. These new technologies will be the thread that ties the sum of the community body of knowledge together.

Summary

Counterintelligence and counterterrorism are the FBI's leading priorities. If we are to successfully mitigate the asymmetrical intelligence threats facing us today and in the future, a new approach, new ways of thinking and better technology are required. We are in the process of redesigning the counterintelligence program at the FBI. It will be much more centralized to ensure the program is nationally directed, prioritized, and that

appropriate management and accountability measures are in place. The Counterintelligence Division will continue to work closely with the Security Division to ensure that our activities are complementary and that the FBI is able to comprehensively address any internal threats. Through our ongoing comprehensive strategic planning process, we are ensuring that our counterintelligence priorities, performance expectations and management practices are designed in a manner that is responsive to ensuring our national objectives are achieved. We are working to not only ensure that counterintelligence personnel have the best possible tools to conduct their work, but also to enhance the training and experience amongst counterintelligence personnel and to bolster counterintelligence as a specialized and vital career within the FBI.

STATEMENT
OF THE
HONORABLE WILLIAM H. WEBSTER
BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
APRIL 9, 2002

Mr. Chairman, thank you for the opportunity to testify before the Committee on behalf of the Commission for the Review of FBI Security Programs. I will keep my opening remarks brief because the Commission's true statement is its report, which I have submitted.

In March 2001, Attorney General John Ashcroft asked me to chair the Commission at the request of FBI Director Freeh. The request came in light of the newly discovered espionage of FBI Special Agent Robert Hanssen. Over the course of twenty-two years, Hanssen gave the Soviet Union and Russia vast quantities of national security information of incalculable value.

The depth of Hanssen's betrayal is shocking, but equally shocking is the ease with which he was able to steal classified material. Usually, Hanssen collected the material during his normal daily routine, gathering up classified information that crossed his desk or arose in conversation with colleagues.

The Commission concluded that internal security has often been a low priority at the Bureau, frequently trumped by operational needs. Security training has been almost non-existent, and agents usually take on security duties as collateral responsibilities, with every incentive to return to investigative operations full-time.

Although it is impossible to eliminate intelligence efforts directed against our national security, the Commission attempted to recommend changes in FBI security programs that will minimize the harm those who betray us can do. The changes should also shorten the time between the defection of these individuals and their detection.

Most globally, the Commission recommends that FBI security programs be consolidated in an Office of Security reporting to the Director. In addition to changes in Bureau policy, we also recommend that a system be established whereby security lapses in a particular intelligence entity lead to improved security measures throughout the entire Intelligence Community.

I would like to acknowledge the support afforded by the Department of Justice and the unstinting cooperation of FBI Director Mueller and Bureau personnel at all levels. The Commission also noted the many steps the Bureau has taken to improve security in light of Hanssen's treason.

Finally, I would like to recognize the dedication of our professional staff and my colleagues on the Commission: Clifford Alexander, Griffin Bell, William Cohen, Robert Fiske, Thomas Foley, and Carla Hills.

I would be pleased to answer your questions.

Addendum to Statement of William H. Webster

Senate Judiciary Committee Hearing
"Reforming the FBI in the 21st Century: The Lessons of the Hanssen Espionage Case"

April 9, 2002
10:00 AM
Dirksen Senate Office Building

Mr. Chairman this concludes my formal statement but I would like to add a few comments of a personal nature before proceeding to respond to your questions.

I am painfully aware that some of Robert Hanssen's activities took place intermittently when I was Director of the FBI. While I worked hard to strengthen its counterintelligence capabilities to detect and capture the spies of hostile countries targeted against us, in hindsight I took our own internal security procedures for granted and I share in that institutional responsibility.

I raised that issue when I was asked to assume this responsibility and was assured that my perspective from nine years at the FBI and four and one-half years at CIA would be useful. With the authority of the Attorney General, I asked six distinguished Americans of unquestionable probity to serve with me as Commissioners and they have joined with me in the conclusions of this Report. I wanted this to be an honest Report and I believe we have produced one.

This Report is not intended to reflect adversely upon the integrity and dedication of the many thousands of men and women who have served their country in the FBI. Indeed, its purpose is to disclose the security vulnerabilities that could have been far more devastating had not the spirit of Fidelity Bravery and Integrity been alive and well for all but a minute number of employees who betrayed their trust.

We owe it to the men and women of the FBI who serve today and will serve tomorrow to address these vulnerabilities in ways that will best protect our country and yet permit the FBI to function fully and effectively in its many responsibilities for the protection of us all.

REFORMING THE FBI IN THE 21ST CENTURY: REORGANIZING AND REFOCUSING THE MISSION

WEDNESDAY, MAY 8, 2002

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, Pursuant to notice, at 2:05 p.m., in room SD–106, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Feinstein, Feingold, Schumer, Durbin, Edwards, Hatch, Grassley, DeWine, and Sessions.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. This hearing marks the continuation of the Judiciary Committee's series of FBI oversight hearings that began last summer. We have considered the report of former Senator John Danforth on the Waco confrontation, the Webster Commission report on FBI security in the wake of the Hanssen espionage case, and the Justice Department Inspector General's report on the disclosure of FBI documents in the Oklahoma City bombing case.

We have heard the important perspectives of FBI agents and senior officials about what they believe the FBI must do to address morale and accountability problems and to improve the Bureau's security counterespionage programs, computer systems, and information management practices. The members of this committee have paid close attention and on April 25 we voted unanimously to report to the full Senate for consideration the FBI Reform Act of 2002, S. 1974.

The risk of catastrophic terrorism, as we know so vividly from 9/11, from the anthrax attacks, and from the threat of a dirty bomb, all of these things have made amply clear that nothing is more critical to the safety of the American people than a well-organized and skillfully managed FBI that uses its vast powers and resources effectively, while adhering always to our Constitution and laws.

The FBI has two key and overlapping missions: protecting our national security by rooting out spies and terrorists, and protecting our public safety by investigating criminal activity. This hearing looks at how the FBI can reorganize and refocus its efforts to perform both missions with the resources made available by the President and the Congress.

You can't plan for the future unless you know what might have gone wrong in the past. That is why I wrote to the Attorney General on October 25, 2001, requesting that relevant material be preserved. On November 8, 2001, I recommended asking Judge Webster's commission to review the FBI's pre-9/11 performance.

While the Attorney General did not commission outside review, this committee has an obligation to understand what happened. Both Attorney General Ashcroft and Director Mueller have assured me that if there is material that turns up as they review that had been overlooked prior to September 11, it will be preserved.

When Judge Webster came before us to describe the deficiencies in FBI security that allowed Robert Hanssen to spy for the Russians undetected for more than 20 years, he described the institutional vulnerabilities of the FBI as "shocking" and "devastating"—this from a man who is a former Federal judge, a former FBI Director, and former CIA Director.

When the Justice Department Inspector General told us that widespread failures by the FBI led to the belated disclosure of documents in the Oklahoma City bombing case, the FBI's current Executive Assistant Director for Administration testified that the Director had made the IG's report "recommended reading for all FBI management and supervisory personnel." I commend Director Mueller for doing that.

In each case, though, before we looked at it, the response was to minimize responsibility. The American public was told Hanssen was "too smart to get caught." The American people were told that computers, not people, caused the delay in the production of documents in the Oklahoma City case.

But the Webster Commission and the IG report made clear that the FBI's security flaws enabled Hanssen's spying, and that bad judgment as well as computers contributed to the production delays in the Oklahoma City case. In both cases, even more than that, a major participating cause was the basic nature of the FBI itself.

We are still in the same position regarding the 9/11 attacks as we were before the Webster Commission and the IG reports. We are told that the conspirators were too clever to have been caught. We are being told the hijackers avoided detection because of meticulous planning and everything else. We hear that nothing short of a member of the inner circle turning himself in would have provided sufficient foresight to prevent the attacks.

Now, these explanations may be actually right, but the American public has a right to ask if they are. There may be more to the 9/11 story than the skill of the enemy, just as there was more to the story of Hanssen than his intellect and more to the story of the Oklahoma City documents than computers.

Press reports say that the FBI failed to pursue pre-9/11 leads effectively, including warnings about two hijackers, and just last week a memorandum of concerns of the FBI's Phoenix office about the possibility of terrorists at U.S. flight schools months before the 9/11 attacks.

The FBI provided the committee a single paragraph from the Phoenix memorandum that recommends that the FBI set up contacts at flight schools and other Government agencies to monitor certain foreign individuals. I hope the Director will help us get to

the bottom of this incident because this is the type of thing I was asking about.

Were there things that the Department of Justice and the FBI overlooked prior to September 11, not to make scapegoats out of people, but to protect us from the next September 11, because the only way you learn is if there was a mistake and if the mistake is admitted and made public and we find out what went wrong and we don't make the same mistake again.

This committee certainly shouldn't be hearing about some of these mistakes coming to light only when we read it in the paper. I am getting somewhat concerned when some of these major things I find, while highly secret, I suppose, I read about on the front page of the New York Times and then I get a briefing subsequently.

As I said before, if that is the way it should be, then each day mark a copy of the New York Times top secret and deliver it to me and I will get the information faster, I will get it in more detail and, of course, I get that wonderful crossword puzzle.

We will want to look at the idea of deemphasizing things at the FBI. Are there too many carjackings, too much domestic violence, too many simple drug possessions, too many driveby shootings? Part of that is our fault; we have Federalized far too many things as it is.

I know the Director is confronting hard decisions about how to refocus the FBI's mission and reorganize the Bureau. We may ask tough questions about those decisions, but if history teaches us anything, it is that asking the tough questions is in the best interests of the American people.

Frankly, Director Mueller, if we didn't have a lot of confidence in you, we wouldn't be spending the time to have these hearings.

I will put the remainder of my statement in the record.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Chairman LEAHY. Mr. Thompson, please feel free to go ahead.

STATEMENT OF HON. LARRY D. THOMPSON, DEPUTY ATTORNEY GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. THOMPSON. Chairman Leahy, members of the committee, thank you for inviting me to appear today to review our progress in strengthening the Federal Bureau of Investigation. This task is among our preeminent and most urgent missions at the Department of Justice because of the FBI's central role in preventing and disrupting terrorist attacks against our homeland.

The Department's success in this effort is critical to restoring the full confidence of the American people in the FBI and to enable the FBI to fulfill its counterterrorism mission and its many other important missions with distinction.

On June 20 of this year, the Attorney General directed the Justice Department's Strategic Management Council to conduct a comprehensive review of the FBI and to make recommendations for reforms. The Strategic Management Council is a group that I chair, composed of senior Justice Department officials, including the FBI Director and heads of other major Justice Department agencies.

The Attorney General gave three specific directives to us in performing this review. First, he directed that a private consulting firm be hired to conduct a management study of the FBI, with particular attention to the issues of information technology, personnel management, crisis management, and performance appraisal.

Second, the Attorney General directed that a wide array of views be solicited from individuals and organizations within and outside the Justice Department, including Congress.

Third, the Attorney General directed that we take into account three other reviews then underway regarding the FBI—the Webster Commission's review of the FBI's internal security practices in the wake of the Hanssen espionage matter, the Inspector General's investigation of that same matter, and the IG's study of the FBI's document-handling procedures in the Oklahoma City bombing case.

As directed, the Department retained a management consulting firm last July to conduct this review. The consultants conducted an extensive analysis of the Bureau, including interviews with a wide variety of FBI personnel and a thorough examination of the FBI's information technology infrastructure. The consultants then submitted a report for consideration by the Department's Strategic Management Council.

To fulfill the Attorney General's directive to solicit a wide range of informed opinion, my staff and I conducted informal interviews with a broad cross-section of individuals, including, among others, former Attorneys General and Deputy Attorneys General, former FBI Directors and Deputy Directors, Members of Congress and their staffs, leaders of organizations representing State and local law enforcement authorities, heads of other Federal law enforcement agencies, and current senior Justice Department officials, including a number of United States Attorneys.

Mr. Chairman, in addition, we have carefully examined the Inspector General's final report concerning the belated production of documents in the Oklahoma City bombing case, as well as the report of the Commission for the Review of FBI Security Programs, chaired by Judge Webster. We anticipate receiving the Inspector General's report concerning the Hanssen case in the next few months, but we have already received preliminary comments from the IG's office regarding FBI internal security practices.

Now, although we began work on this project immediately following the Attorney General's directive in July of 2001, the terrorist attacks of September 11 changed both our timing and our perspective. Those attacks brought into immediate focus the need to intensify our counterterrorism efforts and accord an even higher priority at the FBI to the counterterrorism mission.

Moreover, the attacks caused us to shift our focus from investigating crimes with an eye toward prosecution to detecting, preventing, and disrupting terrorist plans. We are now in the process of developing specific recommendations for the Attorney General, Mr. Chairman. That process is still underway. However, we have not yet formalized our recommendations to the Attorney General.

While Director Mueller already has initiated improvements at the Bureau in a broad range of areas, I would particularly like to commend him for the measures that the FBI has instituted to strengthen its counterterrorism capabilities.

The FBI's Joint Terrorism Task Forces have been expanded to 47 field offices, and by August of this year will be operating in all 56 field offices. The JTTFs have effectively merged the resources of a constellation of Federal, State, and local law enforcement agencies through cooperative information-sharing.

Making use of the PATRIOT Act's provision expanding information-sharing, the FBI now communicates more efficiently and successfully in disseminating critical, time-sensitive information about the threat of terrorist attacks to State and local law enforcement, as well as other Federal agencies.

For example, the FBI's NCIC data base, accessible by over 650,000 State and local law enforcement officers throughout the country, has been expanded to include the names and identifying information of subjects of domestic and foreign terrorism investigations. The FBI is expediting security clearances for appropriate State and local law enforcement officials.

The FBI has also established a new Office of Law Enforcement Coordination to institutionalize information-sharing and coordination with State and local officials. The FBI also has recently established a College of Analytical Studies and an Office of Intelligence, and has committed to hiring more than 100 intelligence analysts to enhance its ability to gather, analyze, and share national security information. In addition, Mr. Chairman, the FBI has already begun to take steps to enhance its internal security procedures and modernize its information technology infrastructure. Once we have completed our review, we will forward our recommendations to the Attorney General.

We look forward to continuing to work together with this committee to sustain the FBI's as our bulwark in the defense of our freedom. This will be a detailed and demanding task requiring a dedication to persevere long beyond September's flush of fury and grief. We at the Department of Justice are committed to this effort, not only to begin it, but to follow through and achieve our goal and the goal of Director Mueller to restore the FBI to its proper place as the preeminent law enforcement agency. Accomplishing this objective is clearly in our national interest.

That concludes my prepared comments and opening statement.

[The prepared statement of Mr. Thompson appears as a submission for the record.]

Chairman LEAHY. Thank you very much.

I think before we start questions, Director Mueller, why don't you go ahead, sir?

STATEMENT OF HON. ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. MUELLER. Thank you, Mr. Chairman. If I could, I want to take a moment just to thank, because I have the opportunity to do so, those who participated in the investigation of the pipe bomber, Helder, who was arrested yesterday, particularly State and local law enforcement, who did just a terrific job together with ATF and other agencies in identifying the person who was responsible and tracking that individual down. I want to thank our colleagues in

State and local law enforcement for the cooperative effort we had in resolving that situation.

Mr. Chairman, the FBI faces daunting challenges from an increasingly volatile world situation. Terrorists at home and abroad threaten U.S. interests at unprecedented levels. Foreign intelligence services continue to target U.S. secrets and technology, often for their own country's economic advantage. Cyberspace is threatened by increasingly malicious criminal activities. Organized crime of all types operates without regard to geographic borders. And, most obvious, the tragic events of September 11 have changed the American landscape forever.

Responding to these challenges requires a redesigned and refocused FBI—imperatives reinforced by the recent findings of Inspector General Fine and Judge Webster. We must refocus our mission and our priorities, and new technologies must be put in place to support new and different operational practices. We must improve how we hire, manage, and train our work force, collaborate with others, and manage, analyze, share, and protect our information. All will be necessary if we are to successfully evolve post-9/11. Most would have been necessary even absent 9/11.

I believe that we all recognize that given the scope and pace of needed change that the FBI is in a period of transformation. This transition is not only organizational and technological, but also cultural. I am more impatient than most, but we must do these things right, not simply fast. Refashioning a large organization takes not only a reformer's zeal, but also a craftsman's patience. The task of transforming the Bureau is a national priority and worth the large expenditure of effort by all of us involved.

Nevertheless, despite the large scope of the challenge, I believe we are making progress on all fronts. I very much appreciate your recent comments, Mr. Chairman, when you said that "The men and women of the FBI are performing the task with great professionalism at home and abroad. Americans have felt safer as a result of the full mobilization of the FBI's dedicated Special Agents, its expert support personnel, and its exceptional technical capabilities," because, as you have indicated, Mr. Chairman, it is our people who are our greatest asset.

Change has many dimensions. We are not only structurally different, but we are fundamentally changing our approach in a number of areas, most notably counterterrorism, counterintelligence, and technology.

As the committee knows, many of these initiatives are works in progress, with final decisions still to come. Currently, I am working closely with Deputy Attorney General Thompson, the Attorney General's Strategic Management Council, and our own executives on all of these issues, and I anticipate being in a position to discuss them in depth with you in the coming weeks. I am also meeting with our Special Agents-In-Charge for the third time next week to consult with them as we continue to work through the complex issues inherent in remaking the FBI.

Central to any successful structural change at the FBI is new technology. As this committee knows from prior hearings, our information infrastructure is far behind current technology and it cannot support the robust analytical capacity we need.

Fortunately, Congress has provided us substantial funding and we are deploying new hardware and networks on an accelerated schedule. Having to so dramatically replace the entire infrastructure rather than make incremental improvements, as is common in the private sector, makes the replacement process more difficult. I am continuing to bring in extremely talented individuals to assist in this endeavor, and will keep Congress regularly advised about both the progress we make and the difficulties we encounter.

Just as we change our technology, we must reshape and retrain our work force. Operating within a culture that most jobs were best done by agents, former Director Freeh began changing that nation and we are accelerating this approach. We are hiring subject matter experts in areas like IT, foreign languages, internal security, area studies, engineering, records, and the like.

There has also been much in the media about coordination with State and municipal authorities, what is commonly referred to as information-sharing. After a series of meetings with our law enforcement colleagues and State homeland security directors, it became clear that our history of solid personal relationships alone was not addressing the basic information needs of our counterparts. They have our attention and we are doing much better. Adding 650,000 officers to our efforts is the only way to make this truly a national effort, not just a Federal effort.

To move forward on this broad range of issues, we took a significant step in the process of change with a major reorganization of the FBI. The first phase established four new Executive Assistant Directors who report directly to me and oversee key areas of our work: counterterrorism and counterintelligence, criminal investigations, law enforcement services, and administration.

This structure should reduce the span of control of the former Deputy Director position, which was a management concern raised here on Capitol Hill and in internal and external reviews of the Bureau. These changes also have increased accountability and strengthened executive-level management of day-to-day operations, and permitted a greater focus on strategic management issues.

This reorganization addressed a number of significant issues, many of them raised before this committee in previous hearings. We created a stand-alone Security Division, headed by an experienced professional from the CIA. We included in the reorganization a Records Management Division, lead by an experienced records expert who also has appeared before this committee.

We also have established an Office of Law Enforcement Coordination that will not only improve relationships and information-sharing with State and local police professionals and others, but will also help the FBI tap into the strengths and the capabilities of our partners. We are hiring High Point, North Carolina, Police Chief Louis Quijas, an experienced executive, to head this new office.

At the same time, the ongoing reorganization responds directly to the events of September 11 by putting a coordinating analytic umbrella over counterterrorism and counterintelligence. The new structure creates the Office of Intelligence, which will focus on building a strategic analysis capability and improving our capacity to gather, analyze, and share critical national security information,

an initiative supported by our new College of Analytical Studies at Quantico.

The continuing reorganization also creates a new Cyber Division dedicated to preventing and responding to high-tech and computer crimes which terrorists around the world are increasingly exploiting to attack America and its allies. Our old approach was fractured and not well-coordinated. This new Cyber Division will move elements of the Criminal Investigative Division and the National Infrastructure Protection Center into one coordinated entity. This change will bring together various cyber initiatives and programs so that we are better focused, organized, and coordinated in working with our public and private sector partners.

We are now in the second phase of our reorganization. As part of this phase, we are developing a comprehensive strategy to permanently shift resources to supplement the substantial new resources Congress has already provided in the fight against terrorism and in support of our prevention effort.

Given the gravity of the current terrorist threat to the United States, the FBI must make the hard decisions to focus its available energies and resources on preventing additional terrorist attacks and protecting our Nation's security.

At the same time, I want to assure you and others in Congress that we will continue to pursue and combat international and national organized criminal groups and enterprises, civil rights violations, major white-collar crime, and serious violent crime, consistent with the available resources and the capabilities of, and in consultation with, our Federal, State, and municipal partners.

We believe the changes to date and those that will be proposed in the near future are vital to ensuring that the FBI effectively satisfies its national security, prevention, and criminal investigative missions. They represent important steps in the difficult process of change.

What emerged from the events of 9/11 leaves no doubt about the need or urgency for change. As you pointed out, Mr. Chairman, in your opening remarks, our investigation of 9/11 paints a sobering portrait of the 19 hijackers and makes clear that they carried out their attacks with meticulous planning, extraordinary secrecy, and extensive knowledge of how America works.

While here, the hijackers did all they could to stay below our radar. They contacted no known terrorist sympathizers, they committed no crimes, they blended into the woodwork. In short, the terrorists managed to exploit loopholes and vulnerabilities in our systems to stay out of sight and to not let anyone know what they were up to, beyond, as you pointed out, a very closed circle.

The patience, skill, and exploitative approach used by the hijackers means that our preventive efforts must be massive, globally collaborative, and supported by ample technology and analytical capability. It means that the information possessed by every agency, both here and abroad, both Federal and local, must go into the multiagency prevention mix and be acted upon.

And it does mean, Mr. Chairman, that we need to look at the lessons of the past and learn from those lessons of the past and make certain that we do not repeat them, and to the extent that there

are organizational or institutional weaknesses or failures, remedy those institutional weaknesses or failures.

Now, in response to 9/11, and with an eye toward preventing future attacks, we have strengthened ties with the Central Intelligence Agency. We have placed key staff in each other's command centers. We are members of the Foreign Terrorist Tracking Task Force, and as I believe the Deputy Attorney General pointed out, we have expanded the number of Joint Terrorism Task Forces around the country, which include both Federal as well as State and municipal officials.

Perhaps as important, within the FBI we have centralized accountability within the counterterrorism program under a new assistant director. Among the new programmatic tools at his disposal will be the Financial Review Group to focus on disrupting the flow of financial resources to terrorists, the Telephone Applications Group, and new data-mining capabilities. We are also establishing flying squads so we have the flexibility to send agents wherever they are needed when a particular threat or crisis arises.

But foremost among the lessons I think we have learned in retrospect is the need for a substantially greater and more centralized analytic capability, resident at headquarters, but available anywhere in the world, available to anyone, anyplace in the world who is combatting terrorism.

We need a capacity with ample resources, better technology and better training, one that is better intertwined with other agencies, domestic and foreign, Federal and local, and all the information that they may possess.

We are designing our new counterterrorism program and technology, standing up an Office of Intelligence, changing our training at Quantico, and hiring subject matter expertise with that exact premise in mind. The capacity must be in place to permit every piece of information from every source to be rapidly evaluated from an analytical perspective.

It is also important, as we search for ways to improve our Nation's capacity to prevent terrorism, for America to look at these attacks in context. The terrorists took advantage of America's strengths and used them against us. They took advantage of the freedoms we accord to our citizens and guests, particularly freedom of movement and freedom of privacy. As long as we continue to treasure our freedoms, we always will run some risk of future attacks.

In addition, the terrorists also took advantage of the openness of our society. Fifty million people, Americans and guests, entered and left America during the month of August 2001, the month preceding the September 11 attack. The vastness of this number highlights the dynamic openness of our society. It is also the source of our economic strength and vitality.

But this openness brings with it vulnerabilities, as 9/11 so terrifyingly showed. America will continue to be free and open, and we at the FBI believe that our job is to protect those freedoms, not reduce them in the cause of security. However, these attacks highlight the need for a different FBI, a more focused FBI, a more technologically adept FBI, an FBI that is more reliant on outside exper-

tise and better equipped to process and use the vast quantities of information available to us.

As I finish, Mr. Chairman, let me just say that I and the 27,000 men and women of the Bureau were as devastated as anybody by the attacks of September 11 and remain deeply affected. But with this has come the conviction to do everything within our power to reduce the risks that Americans run in the exercise of their freedoms.

It is to this goal that all of the reorganization, reform, technology, and new personnel are committed. But ultimately, standing behind all the capabilities that we have now and that we are working to build is a cadre of FBI professionals, men and women who exemplify courage, integrity, respect for the law, and respect for others. We are extremely proud of how they have performed over the past 8 months. As, Mr. Chairman, you have indicated, they have worked long days and nights, sacrificing time with their families to get the job done. It is an honor to appear before this committee representing those 27,000 individuals.

Thank you for according me the time, Mr. Chairman, for my statement.

[The prepared statement of Mr. Mueller appears as a submission for the record.]

Chairman LEAHY. Thank you, Director, and I agree with you; it is an honor to represent them. We have some very fine men and women there. I know many of them, nowhere near as many as you do, but we should be very proud that they are there.

You were on the job less than a week before the 9/11 attacks. You handled that crisis as though you were born to the job, even though that is not the job you wanted to have, none of us wanted to have, anything happening that terrible. I have talked to you a number of times since that day. This is your first formal appearance before the committee and I just wanted to use the opportunity to commend you for the way you have taken charge at the FBI. I also want to commend Attorney General Ashcroft for the support he has given you, and Deputy Attorney General Thompson.

I want to commend the FBI for the swift arrest of the young man who has now been charged with placing pipe bombs in mailboxes across the Midwest.

I appreciate what you said about State and local government and other Federal agencies who work with you. Not only is it a fact, but I know they are going to appreciate you commending them for that.

I know that a lot of postal workers and Americans were vastly relieved when they checked the mail this morning, which made me think of another investigation near and dear to my heart, the anthrax investigation. As I said earlier to you, it is like the Mark Twain character. Now that I have received one of the anthrax letters, and the Mark Twain character being ridden out of town on a rail, if it wasn't for the honor, I would just as soon walk.

I think it is important for the American people, and the Postal Service employees in particular, to know that the FBI is expending enormous resources on finding the murderer who sent the anthrax letters. And that person is a murderer; numerous people have died.

On November 9, the FBI made public a profile of the suspect. Since then, you have engaged the help of the scientific community.

You have collected Ames strain samples from almost 20 sources. You have done hundreds, actually thousands of interviews. You have done genome sequencing, carbon dating, reverse engineering.

Following all the interviews and the tests, have you changed the profile of the suspect that the FBI came out with last November?

Mr. MUELLER. Well, Mr. Chairman, the profile that we came out with then was based on certain information that we had at that time. The results of additional interviews, the results of the tests that we have done to date—many of them are preliminary—have not warranted at this time a revision of that profile.

I should say that as the investigation does on—I am occasionally asked where is the investigation, where are we in the investigation? I want to assure you and the public that it is not in any way stalled. Everyday, we receive new leads with regard to potential individuals, and we have an ongoing, very thorough laboratory investigation undertaken.

Unfortunately, the letter that had most of the anthrax was what has become known as the "Leahy letter," but that has enabled us to conduct tests that, prior to receipt of that letter or finding that letter, we were unable to perform. Those tests are ongoing and are very helpful to the course of the investigation.

I mention the profile because FBI Assistant Director Dwight Adams, the new head of the FBI Lab, has been very helpful to me and my staff. He has explained a lot of the complex tests on the anthrax sample. The FBI has had to rely on scientists familiar with anthrax and bio-weapons research. It is not something that normally—well, to my knowledge, has never come before the Bureau before.

But that may be the same community from which the anthrax murderer comes. He works in a lab, has a scientific background, is comfortable working with extremely hazardous materials, and so on. Some scientists have stated publicly that the perpetrator may be one of their own.

Are we going to have to reach a point where the FBI can develop more of this expertise on its own? And I don't mean that as a criticism, because nobody has ever seen this sort of thing come up before.

Mr. MUELLER. We are in the process of developing our expertise. I will tell you we have changed the recruiting profile, for instance, to include scientists and others with scientific as well as computer backgrounds, for exactly this reason. We are developing our expertise in the laboratory as we go along.

However, with something like this where we come to find that there are various scientists with various views, we have found the best way to obtain the best qualified laboratories and individuals is to pull together a group of individuals highly respected in their fields and attain names from them, and then discuss with particular laboratories and particular scientists the tests that they would perform.

One thinks at the outset of an investigation like this you can go to one scientist and that particular scientist will have all the skills necessary to tell you what you need in order to conduct the investigation. But what we find is you need different skills in different scientists, different areas of expertise to look at the DNA, the ge-

netic makeup, the chemical makeup, and the like. Accordingly, when we are faced with a situation such as this in the future, I think the model that we have developed here is probably the model we will follow in the future.

Chairman LEAHY. Last week, a wire service reported that 2 months before the September 11 attacks, the Phoenix Office of the FBI recommended contacting flight schools nationwide where Middle Easterners might be studying. The FBI has provided the committee a single declassified paragraph from the otherwise classified Phoenix report that recommends the FBI set up contacts with flight schools and other government agencies to monitor certain foreign individuals coming into this country to attend these schools. The paragraph specifically references certain suspicions about how these flight schools were being used.

Can you tell us what the suspicions were and whether any actions were taken in response to the Phoenix report?

Mr. MUELLER. Mr. Chairman, the Phoenix electronic communication contains suggestions from the agent as to steps that should be taken, or he suggested taking to look at other flight schools. It was based on an investigation that this agent and others in Phoenix had conducted and were conducting, and to date is not over.

In the course of that investigation, the agent determined that there were individuals who were looking at flight schools, as well as other airline academies, for a variety of positions; yes, pilots, but also perhaps as roles in security or elsewhere in an airport.

He made a recommendation that we initiate a program to look at flight schools. That was received at headquarters. It was not acted on by September 11. I should say in passing that even if we had followed those suggestions at that time, it would not, given what we know since September 11, have enabled us to prevent the attacks of September 11.

But in the same breath I should say that what we learned from instances such as that is much about the weaknesses of our approach to counterterrorism prior to September 11, and let me spend a moment, if I could, to describe what I perceive to be some of those weaknesses.

First, we in the FBI have been a reactive organization, generally, as opposed to a proactive organization. That comes because we perceive ourselves as being law enforcement. We start from the presumption of we gather evidence and then when we have enough evidence, we arrest people and prosecute them. In the future, we have to be more proactive. We cannot wait until we have evidence of a crime having been committed, but have to take what evidence we have and make predictive observations to avoid the next attack.

Second, one of the lessons learned is that we are a dispersed organization. Our headquarters in the past has been a coordinating entity, with our SACs and the agents in the field doing all of the investigation. In the future, we have to particularly centralize intelligence-gathering, intelligence analysis, and intelligence dissemination from headquarters, which brings me to the third thing.

Prior to September 11, we did not focus as we should on our analytical capability, understanding that we have to take every piece that may be provided to us and put it in a larger framework, in a larger puzzle.

We have changed dramatically to address some of these shortcomings. We have beefed up headquarters, with the understanding that the Counterterrorism Division and the Assistant Director must not just coordinate, but direct and manage investigations in the future, so that when something like this occurs, when there is a suggestion made, we would then pursue it, and pursue it aggressively. We have beefed up our analytical capability, which includes individuals, analysts, and have sought even more analysts. Part of beefing up our analytical capability quite obviously is the technology which we also have sought. So we have used instances like this in order to try to reshape and redefine how we address counterterrorism.

Chairman LEAHY. I will come back to this, and I have some questions for General Thompson, too, but I will yield to Senator DeWine, going on the usual early bird rule.

Senator DEWINE. Thank you, Mr. Chairman. I do have to go to the Intelligence Committee. I appreciate it very much.

Thank you for joining us. We appreciate it very much. We appreciate the work that both of you are doing.

Mr. Director, you and your team are really redefining the role of the FBI. I don't know of any FBI reorganization in my lifetime that that has shifted the FBI's focus to such an extent.

I think as you lead this change that your natural inclination for candor will work to your advantage because you are faced with setting priorities every single day. You have had to already make some horribly difficult and tough choices.

I think, though, that it is very important for you to continue, to involve the American people in that debate and that setting of priorities. As you shift thousands of agents to this new war effort and as the posture of the FBI changes, maybe forever, there are going to be things that simply will not get done. I think it is important for this Congress to know what is not getting done and for the American people to know what is not getting done.

My information would indicate that your work on white-collar crime, for example, is not getting done to the extent that it previouly was being done. My information would indicate to me that, in the area of anti-drug efforts, you are not able to do what has been done in the past.

When you are dealing with the anti-drug problem, the American people may say, well, local law enforcement can do that. They do that every day. We know that. But what is important for the American people to understand, and what I would like you to comment on, is the unintended consequence of shifting resources away from the long-term work that your Department does on drug cases—you are the ones who do the long-term work with informants and work these cases for months and months, and sometimes for years. That work leads you and other law enforcement agencies to identify other violent criminals. So you are not going to be able to get to those violent criminals because you are not doing the drug work.

I would just like you to comment on that. I don't have any problem with where you are going with priorities, but I think we all need to know what the consequences of these decisions are. I would just like for you to comment and if you disagree with the premise, please say so, as I know you will.

Mr. MUELLER. Starting off with your noting that we have not been doing particularly since September 11 all that we had been doing in white-collar crime and narcotics prior to September 11, that absolutely is true because the investigation after September 11 required almost half of our agent population.

I mean, we had approximately 6,000 agents working on the investigation in the weeks and immediate months following September 11. We also put together a substantial task force operating out of Washington, D.C., to address the anthrax threats. That quite clearly has meant that agents who would be doing other things would not be able to work on, say, white-collar or other types of programs.

I will tell you that since September 11, as we have run through in excess of 300,000 leads, the numbers assigned to counterterrorism have dropped rather dramatically and we are currently down to around 4,000, maybe 3,500 to 4,000 that are still working terrorism matters.

What I have been engaged in for several months is looking at a three-stage process and reassigning resources, it seems to me, that we need to determine exactly what number of resources we need to address counterterrorism around the Nation. I have sought the input and received the input from the special agents-in-charge of the various divisions so that I know what in their minds they think they need to discharge the counterterrorism responsibilities. It goes without saying, however, that to the extent that we have any lead in counterterrorism that should be followed up, every SAC should make that the first priority regardless of what we do down the road.

The first part of the process or the equation was to determine how many additional agents we need to do counterterrorism. Once that is done, I have to look at each of the programs, with the help of the SACs, to determine from whence those agents come.

The last part of that process is if we are going to take agents from one of those programs, who is going to pick up the slack, who is going to fill the void that is left by our moving to another program, which requires conversations and consultation not only with State and local law enforcement but our other Federal partners, as well as Congress.

I am at the latter stages of that process, so I would expect in the next couple of weeks, two to 3 weeks, to be back up here talking with various Members of Congress to give you an indication as to where I think these additional resources should come from. But I see it as a three-tiered process, I guess I should say.

The other thing I should point out is I am somewhat reluctant to make wholesale shifts between offices, for instance, because I have experienced in the past, where there is a crisis or a challenge, we may have thrown agents at that challenge and once the challenge is met those agents stay where they are.

I am reminded of the savings and loan scandal, where we had agents back in the early 1990's that went to Dallas and other places. Many of those agents are still there, although the need is not there. Consequently, I want to make certain that when we reassign agents to different programs, to counterterrorism, we do know who is going to be picking up the slack and they will have

worthwhile tasks to perform, and that we ought to be flexible down on the road in adjusting.

That is, in broad view, my philosophy as we go through this process.

Senator DEWINE. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Grassley had to go back to another hearing. He did want me to make these three sentences for him. He wanted to thank you, Director Mueller, and the FBI for the way you handled the investigation of the pipe bomb cases. Senator Grassley said the bombs injured a number of people in his home State of Iowa, and he is grateful and pleased that the FBI could wrap this up and get a suspect in custody. Senator Grassley said further that he appreciated the call you made to him yesterday, letting him know what was going on.

The Senator from California.

Senator FEINSTEIN. Thanks very much, Mr. Leahy.

Good afternoon, Mr. Mueller, Mr. Thompson. I think you know, Mr. Mueller, I have a very great respect for you. You are straightforward and direct and there aren't any artifices, and I for one really appreciate that.

I think you know that yesterday I sent you a letter asking some questions about this electronic communication known as the Phoenix memorandum, and I would like to ask you some questions about it. As I member of Intelligence, I have read a copy of the original electronic communication and I must tell you that it strikes me as something that does not require a great deal of analysis. It is what it is, it is very straightforward.

In the reports that I read in Intelligence, it is much more consequential than many of them that I read on almost a daily basis now, much fuller, much more descriptive. So I would like to ask just a few questions from my letter, but before I do, Mr. Chairman, I would like to ask that this letter, dated May 7 to Mr. Mueller, be placed in the record, if I might.

Chairman LEAHY. Without objection.

Senator FEINSTEIN. Let me begin with the first question on it. Who, by name and title, within the FBI was provided this electronic communication? Was the EC or its contents brought to the attention of the Director of the FBI? If so, when. If not, who was the highest ranking FBI official made aware of the EC or its contents?

Mr. MUELLER. Senator, let me just say I received a copy of your letter this morning and I glanced through it. To the extent that I can answer the questions, quite obviously I will.

Senator FEINSTEIN. I understand that.

Mr. MUELLER. But there is a lot that you request in terms of information that I am not on top of.

Senator FEINSTEIN. I understand, I understand.

Mr. MUELLER. I am not certain as to the highest-level individual who received it. I do not believe at this juncture that it went so high as the Director of the FBI, but I am not certain how high it went in the hierarchy. I think that was the thrust of that first question.

Senator FEINSTEIN. Right. Now, the reason I am asking the questions that I am is not to be critical, because it is very easy to be a Monday morning quarterback, but to say when something like this comes through let's look at the process that governs it because clearly a lot of things could have happened with that. In my judgment, it is something that perhaps should have gone right to the Director of the FBI, and perhaps he should have even sent it to the President.

Let me ask another question. It is my understanding that the standard method by which the FBI disseminates intelligence is by way of a letterhead memorandum, often called an LHM. Was an LHM drafted based on the information contained in the EC, and if not, why not?

Mr. MUELLER. Let me again caution my remarks by saying I am not certain. I have not seen all the paperwork with regard to that EC. I quite obviously have seen the EC. In terms of whether there was a letterhead memorandum, I am not aware of a letterhead memorandum that had been prepared, but I am not certain that the premise that intelligence information is only distributed by letterhead memorandum is accurate also.

I have seen that intelligence information quite often is distributed by way of EC. So I am not certain that there was a letterhead memorandum, but I am not certain that that makes some difference.

Senator FEINSTEIN. All right.

Mr. MUELLER. Could I respond to one thing in terms of the procedures?

Senator FEINSTEIN. Absolutely.

Mr. MUELLER. I think it important—I know you have seen the full letter—to understand that the individuals who were mentioned in that letter, and there were a number, were, and perhaps some may continue to be under investigation. So I just wanted to point that out as we continue this dialog.

Senator FEINSTEIN. I am not going to state what was in that at all.

Let me ask you this question: Was the EC or information in the EC provided to FBI personnel assigned to the Director of Central Intelligence's Counterterrorism Center?

Mr. MUELLER. Before September 11, I do not believe so, but I am not certain on that. But I do not believe so.

Senator FEINSTEIN. I think that this is a very worthwhile exercise to go through this because I suspect that nothing happened with it. Now, having said that, the question then becomes, well, what should have happened to this and how many other things perhaps are falling between the cracks.

Particularly after Mr. Moussaoui was arrested, which happened a month after this, it should have been a real signal that something was going on. Then, about the same time as the Phoenix memo, United States intelligence—I guess the CIA—issued a warning that there was a heightened risk of a terrorist attack on Americans, possibly on U.S. soil.

So there were two things out there that should have alerted something in the system to these. At the very least, run them through State's data base, see where the visas came from, see how

many visas are out and where they are to people in similar circumstances.

I think if it did drop between the cracks, I think there is a serious problem because if one thing drops, others probably have as well. That is why I think this is an instructive exercise. I mean, if I had seen that, I would have sent it right to the President. I feel that strongly about this kind of thing.

I think the more I read in open-source information about the FBI at this period, particularly books on terrorism in this country, one of them by Stephen Emerson, for whom I have a great deal of respect, the FBI was very much constrained in what it did and in how it acted. I found some of the things in the book really surprising.

I just wonder if you have any comment. Have you looked at that memo as to where it went at all and what happened with it?

Mr. MUELLER. Yes.

Senator FEINSTEIN. Can you tell us anything about how it was treated?

Mr. MUELLER. Well, it was my understanding again—and we are providing every document, as you well know, to the Intelligence Committee on that. My understanding is that it was in the section, it was looked at in the section. I believe the agent was aggressive, was good, and the suggestion was a good one.

It was a monumental undertaking. There are more than 2,000 aviation academies in the United States. The latest figure I think I heard is something like 20,000 students attending them, and it was perceived that this would be a monumental undertaking, without any specificity as to particular persons. The individuals who were being investigated by that agent in Phoenix were not the individuals that were involved in the September 11 attack.

All that put aside for a second, though, it is a very worthwhile process and a process we are undertaking to change what we do in response to that instance and others where perhaps we did not have the analytical capability, we did not have the people who were looking at the broader picture to put the pieces in place. That is how we have to change.

We are, as I said a few moments ago, and have been, a law enforcement agency and we have been more reactive than proactive. We have not built up the intelligence capacity or capability as we should. One of the things we are doing is putting in an Intelligence Office, and I have requested from George Tenant an individual from CIA to head it up. That provides two things to us. One, it provides us a person who is experienced in intelligence-gathering, analysis, and then dissemination. It also links us better than we have been in the past with the CIA.

So do I wish that we had more aggressively followed up on that suggestion at the time? Yes. Are we taking steps to address what the failings or weaknesses were prior to September 11? Absolutely.

Senator FEINSTEIN. Thank you. My time has expired. Thank you.

Chairman LEAHY. Senator Edwards?

Senator EDWARDS. Thank you, Mr. Chairman.

Mr. Director, I join my colleagues. We all have enormous respect for you and appreciate very much the job you are doing.

I also want to ask you about the Phoenix memo, recognizing, of course, that you weren't there at the time. First of all, I think that the American people are entitled to know why it appears at least that red flags were ignored before September 11, and I think the FBI has a lot of explaining to do. I think our responsibility is to sort of get to the bottom of this and find out what happened. Let me just followup on some of Senator Feinstein's questions.

As I understand it, the memo, to the best of you knowledge, never went as high as the FBI Director. Is that correct?

Mr. MUELLER. I have not asked Louis Freeh whether he saw it. I do not believe it went to the Director, no.

Senator EDWARDS. And it also didn't go to the CIA Director. Is that correct?

Mr. MUELLER. I do not believe it did.

Senator EDWARDS. Now, when the Moussaoui investigation began a month or so later, after July—I think it began in August of 2001—did that arrest in August lead to any renewed response to the Phoenix memo?

Mr. MUELLER. I am not certain whether at headquarters somebody said this is the same type of thing. I am not certain what the agent did in Arizona. To the extent that you are asking whether there was any additional effort made on flight schools as a result of putting Moussaoui together with the Phoenix EC, I do not believe that to be the case.

I believe we looked at the Moussaoui case as a red flag. I mean, one of the red flags you talk about was Moussaoui, and we go out and at the response of the Pan Am flight academy—and they had found him to be somewhat difficult and different, and called up the FBI—we go out and interview Moussaoui and we have no basis to arrest Moussaoui. He has committed no crime.

He is a student who is a little bit odd in the course of what he is trying to do, and the only way that we can address Mr. Moussaoui is to find that he has overstayed his welcome in the United States, is out of status, and we have INS arrest him. So red flags went up.

The agent in Minneapolis did a terrific job in pushing as hard as he could to do everything we possibly could with Moussaoui. But did we discern from that that there was a plot that would have led us to September 11? No, I rather doubt it. But should we have done more in terms of the Phoenix EC? Yes.

Senator EDWARDS. Well, I think one of our responsibilities is to determine what you could have figured out based upon followup that didn't happen, as it turns out.

But if I understand it correctly, you got the memo in July from Phoenix making specific recommendations. About a month later, the Moussaoui investigation and arrest occurred, roughly a month later, relating to a similar topic, obviously. The Director of the FBI, to the best of your knowledge, didn't know about the Phoenix memo. The Director of the CIA did not know about it. Is that all accurate?

Mr. MUELLER. I think that is accurate.

Senator EDWARDS. OK.

Mr. MUELLER. I will tell you I think that is accurate because I have not followed the trace of——

Senator EDWARDS. If that turns out not to be true, would you let us know that, please?

Mr. MUELLER. Sure.

Senator EDWARDS. I also am a member of the Intelligence Committee and I have seen the memorandum, and I also believe that it at least appears to have been an enormous red flag.

Let me ask you about three things that were reported in the newspaper about the memo and get you to respond to them, if I can. First, and this is from the New York, it says "Phoenix believes that the FBI should accumulate a listing of civil aviation universities and colleges from around the country," and I am quoting from the newspaper now.

Did the FBI do that?

Mr. MUELLER. Not to my knowledge, until after September 11. It did, after September 11, but not before September 11.

Senator EDWARDS. Not before September 11.

Second, "FBI field offices with these types of schools in their areas should establish the appropriate liaison." Did the FBI do that before September 11?

Mr. MUELLER. After September 11, not before.

Senator EDWARDS. But not before?

Mr. MUELLER. Not to my knowledge.

Senator EDWARDS. Third, "FBI headquarters should discuss this matter with other elements of the U.S. intelligence community and task the community for any information that supports Phoenix's suspicions." Did the FBI do that?

Mr. MUELLER. That, I am not certain about, at what level. I am not certain about that.

Senator EDWARDS. You indicated earlier that the Director of the CIA didn't know about it. But you think there is a possibility something else occurred?

Mr. MUELLER. It is a possibility, but I would only say a possibility that somebody down the chain had conversations with persons at the CIA. I just don't know whether that happened or not.

Senator EDWARDS. The FBI has said in a statement, and you have indicated something similar to this today, that none of the people identified by Phoenix are connected to the 9/11 attacks. That is, I assume, accurate and a fairly narrow statement.

Did any of those people have any connections to Osama Bin Laden or any terrorist groups?

Mr. MUELLER. The persons who were being investigated by the agent in Phoenix?

Senator EDWARDS. Correct, that is the question.

Mr. MUELLER. I am not certain without going back and looking and checking. There were a number of individuals that were listed in that EC and I am not certain. I cannot recall.

Senator EDWARDS. Whether they are connected to Bin Laden or whether they are connected to any terrorist group, you don't remember either one?

Mr. MUELLER. Well, I know that we believed that one or more were connected with terrorist groups.

Senator EDWARDS. But you are not sure whether it was Bin Laden?

Mr. MUELLER. I am not certain whether it was specifically Al-Qaeda or Bin Laden.

Senator EDWARDS. Are those people still at large?

Mr. MUELLER. I hate to get into it in open forum. Let me just put it that way. I would be happy to answer that——

Senator EDWARDS. That is fine. I accept that.

Well, Mr. Director, thank you for being here. We appreciate your answers to these questions. I hope you can understand why we are concerned about this, obviously with the magnitude of what happened and the information that was apparently available both in July and then in August, before the attacks.

I do believe we have a responsibility to get to the bottom of this, and we appreciate your help with it. I know you also want to get to the bottom of it.

Mr. MUELLER. We share every interest in seeing what happened, what lessons are to be learned, so we do not repeat those lessons. We are making every effort to cooperate and fully disclose anything and everything to the Joint Committee.

Senator EDWARDS. Thank you, Mr. Director.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman.

Chairman LEAHY. I believe you came in first. Senator Durbin is next, I want you to know.

Senator FEINGOLD. Thank you, Mr. Chairman, for your leadership and for holding a hearing on this important subject.

Deputy Attorney General and Director Mueller, thank you for joining us today. I sincerely want to thank you for your long hours and hard work, particularly since September 11. It is important that you are here to discuss with us how the administration plans to reorganize the FBI to use its resources and skills most effectively to attend to the greatest criminal and national security threats to our Nation.

Before I get to my questions, and since the Deputy Attorney General is with us today, I would like to take this opportunity to reiterate here on the record that I hope he, the Attorney General, and President Bush are still committed to ending racial profiling.

It has been more than a year since President Bush pledged to end racial profiling, and it is almost 1 year since Representative Conyers and I introduced legislation, the End Racial Profiling Act.

Mr. Thompson, we have talked about this before and you have made some very powerful statements on it. I would request from the Department an update on the status of its deliberations on our bill and whether it remains committed to a ban on racial profiling. This is more of a request than a question, but if you would like to respond briefly, I would like you to do that at this time.

Mr. THOMPSON. Senator Feingold, I can assure you that the Department, and specifically the Attorney General and myself, remain committed to doing everything we possibly can to eliminate racial profiling, to eliminate race being used as a basis for law enforcement actions. You and I have discussed that in the past.

We are working hard to bring to fruition our studies with respect to racial profiling at the Federal level. Since 9/11, our efforts have

required some updating and we are in the process of getting that completed, but we are not standing still with respect to this important topic. The Department is committed and is actively taking a leadership role with respect to racial profiling at the operational law enforcement level, with respect to providing training to Federal agencies, with respect to data collection, the use of race as a factor in law enforcement actions.

So we hope to complete our studies in as timely a manner as possible, and we will get to the conclusion of this, I can assure you.

Senator FEINGOLD. Do you still support a ban on racial profiling?

Mr. THOMPSON. Yes, sir.

Senator FEINGOLD. Well, good. I don't see any reason why we can't work together to get a bill to the President's desk.

Mr. THOMPSON. We look forward to working with you.

Senator FEINGOLD. Very good.

I would also like to tell you about another matter. Director Mueller, I understand that, a part of the FBI's renewed focused on antiterrorism is the creation and maintenance of a so-called watch list of potential terrorists, and I want to tell you about an incident in Wisconsin a few weeks ago.

A group of close to 40 peace activists were planning to travel to Washington, D.C., to participate in workshops and demonstrations. I understand that as the members of the group were checking in at the Milwaukee Airport, at least one person and possibly more apparently triggered a possible match on the watch list. And because at least 20 members of the group had bought their tickets together and the possible match was triggered by someone in that group of 20, all 20 travelers were detained for questioning.

It turns out that none of the members were determined to be security threats and all were ultimately cleared to fly. Unfortunately, these passengers were scheduled to be on the last flight to Washington for that day, and because it took so long to clear the passengers, some of these passengers missed their flight and had to wait until the next morning to travel here.

Now, of course, we all recognize that we need increased security measures at our Nation's airports and all passengers are understandably enduring some inconvenience and longer wait times before boarding their flights. Nonetheless, I think the incident does raise some concerns.

How, if you could tell me, could these Wisconsin residents trigger the watch list? Can you assure this committee and the American people that the FBI has not and will not include on the watch list persons who exercise their lawful rights of free speech and freedom of association to express their views that may be at odds with the policies of the U.S. Government?

Mr. MUELLER. Well, as to the last statement, absolutely I can assure you, Senator, and the American public that we would never put a person on the watch list solely because they sought to express their First Amendment rights and their views.

With regard to that incident, I am not familiar with the details as to why one or more of those individuals was on the "no fly" list. There are a number of participants and contributors to that. I will tell you from the perspective of the FBI, prior to September 11 we had no mechanism for alerting State and local law enforcement

that there were individuals in the country for whom we had no paper, we have no arrent warrant, they have no crime triggering an arrest piece of paper. Nonetheless, we believe they are an individual or individuals that we need to talk to because we have gotten intelligence from the CIA or elsewhere that they may be associated with terrorism.

We needed some mechanism to alert State and locals. We have used NCIC to do so, understanding that it is critically important that we have State and locals identify a person has been stopped, not necessarily detained, but get us the information that the person has been stopped at a particular place.

We are very careful, once we have interviewed a person we need to interview because we have information that they may be associated with a terrorist or have information relating to a terrorist, that the name be removed from the watch list. It is important for us to have some mechanism to try to find individuals within the United States who may be committing terrorist acts.

On the other hand, we understand the responsibility of making certain that once a person is interviewed, they are removed from the watch list, and that we have various gradations on the watch list depending on the threat and depending on whether there is any paper outstanding on the individual.

Senator FEINGOLD. I think following that a little bit in terms of these lists, do they contain only the names of the suspected terrorists? If so, how does the FBI define who is a terrorist for purposes of determining whether somebody should be placed on the list? Just give me a sense of what the factors are to determine if somebody should be on the list.

Mr. MUELLER. Well, I am going to tell you that prior to September 11 there were two individuals, and the CIA gave us the names of these two individuals and said that they had been at a meeting in Kuala Lumpur with known terrorists and we needed to find them. They actually happened to be two of the hijackers, as it turns out. They came through immigration, they say, staying at Marriott in New York City. Well, that does us no good. We have no mechanism to try to identify those persons.

Senator FEINGOLD. So it is as narrow as being at the January 2000 meeting in Kuala Lumpur?

Mr. MUELLER. With terrorists, yes, with terrorists.

Senator FEINGOLD. What would be the other category?

Mr. MUELLER. You can have associates of terrorists, in the wake of September 11, for instance.

Senator FEINGOLD. How do you define "associates of terrorists?"

Mr. MUELLER. Well, in the wake of September 11, we go to the flight schools and say, OK, this individual was a hijacker. Who were the friends? Were there any companions that he hung around with? If there were, we want to identify them. We want to know whether that individual is in the United States contemplating a terrorist act.

The only way we can identify that person is that person is stopped, but we put in identifying—there are differences in names, but where we have it—and I would say in 99 out of 100 circumstances we put in dates of birth, information that we gather

from the passports as they come into the United States so that there is some specificity.

Senator FEINGOLD. I appreciate that. Let me just ask, does the FBI have a procedure for helping airline security quickly determine if someone whose name comes up on a list is actually the person that the FBI intends for security to stop?

I understand in this instance, at least one analysis of this instance was that it was just that somebody's name was similar to somebody else's name.

Mr. MUELLER. Well, we have a 24-hour watch that is the recipient of telephone calls, but it may not be the FBI. Other agencies also have persons that they put, for a variety of reasons, on the watch list, not just the FBI.

Senator FEINGOLD. I guess my time is up. I will come back on another round.

Chairman LEAHY. Thank you.

Senator Durbin?

Senator DURBIN. Thank you very much, Mr. Chairman.

General Thompson and Director Mueller, thank you for joining us. I want to return to this Phoenix memo. I am very troubled by this and I think that it is likely to become a major concern for Americans because in my committees on Capitol Hill we have been assured and reassured that the tragedy of September 11 was unanticipated. It came as a startling surprise to those who followed terrorist activities, and it was understandable because our theory about hijacking for the longest time had been be submissive, be cooperative, and everything will work out. We came to learn on September 11 that we were just plain wrong.

Let me go back to this Phoenix memo, if I can, and I believe a question was asked earlier, did the FBI agent in Phoenix in communicating this memo link any of his concerns with Osama Bin Laden?

Mr. MUELLER. I am not certain of that. I would have to go back and read that memorandum.

Senator DURBIN. If such a linkage were made, would you agree that the Office of Counterterrorism should have paid special attention to that memorandum?

Mr. MUELLER. I think the Counterterrorism Section should have—it did pay some special attention to that memorandum. There were specifics in there that required further investigation, at least one other office. That other office was alerted. I would agree that it should have disclosed that memorandum or discussed that memorandum with the CIA.

Senator DURBIN. But that was done, to your knowledge?

Mr. MUELLER. I do not know whether that was done at a lower level.

Senator DURBIN. Director Mueller, will you be releasing this memorandum?

Mr. MUELLER. It is still a classified memorandum. There are aspects of the memorandum that, in my view, still should remain classified because it is an ongoing investigation. The memorandum in full has been disclosed to the Intelligence Committee. In terms of releasing the memorandum, publicizing it, no, I would not support that.

Senator DURBIN. Would you release a redacted form of this memorandum?

Mr. MUELLER. We have released, I believe, and sought declassification of that which I think we can. In other words, there is a paragraph of it that I know has been released. I am not certain whether there are any other areas of it that can. We would have to look at that and get back to you.

Senator DURBIN. But the FBI, the Department of Justice, or some other agency, to your knowledge, actually contacted the press for this May 4 story that was reported in several newspapers about the memorandum?

Mr. MUELLER. Contact and trigger the——

Senator DURBIN. Yes.

Mr. MUELLER. No, not to my knowledge. No. I want to say no. It came as some surprise.

Senator DURBIN. Do you believe as you testify today that the FBI ignored a clear warning about the pending events of September 11 by not responding properly to this memorandum?

Mr. MUELLER. Yes, I would disagree with that statement. I think the recommendations of the agent are something that we should have more aggressively pursued. I do not believe that it gave the sign post to that which would happen on September 11.

Of the warnings that we had, the stopping of Moussaoui, the arrest of Moussaoui, brought the Bureau, and particularly the agent in Minneapolis, to the belief that this individual is the type of individual that could and might be the type of individual to take a plane and hijack it. In fact, if I am not mistaken, in one of the notes, the agent in Minneapolis mentioned the possibility of Moussaoui being that type of person that could fly something into the World Trade Center.

Senator DURBIN. Press reports focus on Embry Riddell University in Prescott, Arizona, as the concern of this Phoenix agent. Certainly, Moussaoui was involved in another aviation school, if I am not mistaken.

Mr. MUELLER. In which one?

Senator DURBIN. Moussaoui was involved in training at another school.

Mr. MUELLER. Yes, that is correct.

Senator DURBIN. So the FBI felt within a few weeks that taking action against Moussaoui at another school was appropriate. Was that memo taken into consideration, do you believe, in that decision?

Mr. MUELLER. I am sorry. Which decision would that be?

Senator DURBIN. The decision to pursue Moussaoui, to arrest him.

Mr. MUELLER. I don't believe the Arizona EC was factored—I am not certain, but I do not believe the Arizona EC factored into the decision to arrest Moussaoui. It was the agent who went out to Pan Am aviation school who determined that this person presented a threat, had no basis to arrest this person, but saw that he was out of status and asked the INS to arrest him.

Senator DURBIN. I want to reiterate that I know that this happened before you were in your position of leadership, but I think it reflects on what we are discussing today, the process at the FBI

and how it has been pursued. I believe the Phoenix memo is going to come to be one of the most important documents in our national debate about whether we did enough to protect America from the attacks of September 11.

It strikes me that a memo coming from an agent of the FBI to the counterterrorism office in Washington which identifies concerns about terrorists and their linkage to other terrorist organizations involved in aviation training, and calls on the agency to move quickly to respond at several different levels with limited impact, limited effect, from what we hear today, is going to be a source of further investigation and concern.

I urge you, if it is possible, to release this memo, even in redacted form, so that there is no element of concern that we are not being frank and candid with the American people about what happened. I hope that you will consider that.

Mr. MUELLER. I will.

Senator DURBIN. Thank you. Thank you, Mr. Chairman.

Chairman LEAHY. I would note that this committee made that request about a week ago of the FBI. We are still waiting and hope at the very least we can make it available to members.

Director, in addition to the Phoenix memo, the press reported that Filipino authorities alerted the FBI as early as 1995 that at least one of the Middle Eastern pilots who trained at American flight schools had proposed hijacking a commercial jet and crashing it into Federal buildings. A month before 9/11, the FBI arrested Zacarias Moussaoui as a result of his suspicious behavior at a flight school.

Was the information in the Phoenix report or the information provided by the Filipino authorities in 1995 considered by the FBI when it was determining whether to seek a FISA search authority on Moussaoui?

Mr. MUELLER. I am not certain about that, Mr. Chairman.

Chairman LEAHY. Do you suppose we can get an answer on that for the record?

Mr. MUELLER. Sure.

Chairman LEAHY. We can discuss whether we could get FISA or not, but I would think that if the press reports are accurate about the information provided by the Filipino authorities, that is something that should have been considered.

Mr. Thompson, I noticed that twice in your testimony you referred to an expensive and extensive study done by what you call a private consulting firm and a management consulting firm. Actually, the unnamed firm is Arthur Andersen, the same Arthur Andersen that is prosecuted by the Department of Justice in a Texas courtroom today.

While the Attorney General has recused himself from that, and appropriately so, you have not, and also appropriately so. So I am going to ask you a few questions.

I was concerned about Arthur Andersen in early January and asked about the role Arthur Andersen played in the Department's review of the FBI. The Department's response in February stated that only the audit practice was under investigation, not the consulting practice used for the FBI review.

Shortly after Arthur Andersen had completed its work on the FBI, on December 14 OMB asked the General Services Administration to determine whether to allow Arthur Andersen to continue doing business with the Government. In the end, both Arthur Andersen's consulting and auditing practices were suspended from further Government work based upon its unsatisfactory record of integrity and business ethics.

What reliance, if any, are you placing on the Arthur Andersen report as you move forward with FBI reorganization?

Mr. THOMPSON. Mr. Chairman, let me just briefly explain to you the background by which Arthur Andersen was selected to participate in our review, if that would be helpful.

Chairman LEAHY. They were selected prior to the Enron debacle.

Mr. THOMPSON. That is correct.

Chairman LEAHY. I understand that, but what reliance are we having on their report today?

Mr. THOMPSON. We are relying on certain aspects of the Andersen report. The Attorney General also asked us to review a number of other reports and to undertake a number of other steps in coming to conclusions, and taking into consideration, before we made our recommendations to him.

For example, Mr. Chairman, he asked us to consider the report of the Webster Commission. He asked us to consider the two IG reports, the one that dealt with the Oklahoma City bombing documents and the one that dealt with the internal security problems of the FBI in the wake of the Hanssen matter. As you know, he also asked us to conduct interviews of individuals both within the Department of Justice and outside of the Department of Justice, including Members of Congress.

So the Andersen report, which was completed before the issues of the Enron investigation arose—the Andersen report, along with the other documents and studies and our interviews, will all be considered in our recommendations to the Attorney General.

Chairman LEAHY. So the Andersen report will be one of the things you rely on?

Mr. THOMPSON. Yes, sir.

Chairman LEAHY. The FBI Reform Act codifies the Attorney General's decision last year to authorize the Justice Department Inspector General to investigate cases of FBI misconduct. The FBI Office of Professional Responsibility would still have an extremely important role. The Office of Professional Responsibility, OPR, would continue to investigate FBI misconduct allegations, especially those the IG chose not to handle.

But they also make crucial recommendations, Director, to you on disciplinary sanctions, and so OPR leadership is important because of the message it sends throughout the FBI. Last year, several FBI officials who had sterling records of ethical integrity described these problems at a committee oversight hearing, and their courage and devotion to the Bureau's interests were extraordinary. I got letters, calls, e-mails, and so on, from agents all over the country praising them.

What are your views on the need for OPR leadership to send the right ethical signals throughout the Bureau?

Mr. MUELLER. It is critically important that we have an OPR, what in a police department would be an internal affairs unit, that is perceived as being fair, is fair, and therefore perceived as being fair, expeditious. That is one of the things that I am looking at.

I believe that in looking at the workload, we have taken too long to resolve certain cases. We are looking at the possibility of delegating some of the smaller issues to the SACs to free up OPR to work on cases more quickly and get the resolutions resolved as quickly as possible.

We have tried to eliminate any discrepancies between the handling of cases, whether it be an agent or somebody in the SES, and we are still working at that. But it is critically important that OPR be, and be perceived as, fair and expeditious.

Chairman LEAHY. Thank you. I have other questions, but Senator Schumer is here.

Senator Sessions, did you want to ask questions?

Senator SESSIONS. Yes.

Chairman LEAHY. Go ahead.

Senator SESSIONS. Mr. Chairman, I appreciate the opportunity to ask a few questions.

It is great to see two fine citizens before us, Larry Thompson and Bob Mueller. No government could have finer public servants than they, or have the experience and background and do the job that they do. I know, as Deputy Attorney General, Mr. Thompson has to deal with a lot of frustrating issues, trying to get people to agree and work together. But he has the skills to do that, and proved that as United States Attorney in Atlanta, and I had the opportunity to work with him. My admiration for Mr. Mueller is unbounded as a career professional prosecutor of the highest order.

Mr. Thompson, you remember, I am sure, when President Reagan appointed William French Smith as Attorney General, and the Associate Attorney General was Rudy Giuliani and he established law enforcement coordinating committees. That was a direction to the United States Attorneys and all Federal agencies to work with local agencies, to have meetings and a formal committee to identify the law enforcement priorities in that district and to focus on those priorities. In other words, use the Federal resources within the area to the highest priorities of the area, somewhat diminishing the idea that everything should be decided in Washington.

I thought that was a great success. I think you thought so, too, so I will ask if you are troubled by the priorities appearing to be awfully tough from the top of the FBI down.

Mr. THOMPSON. Senator Sessions, I do agree that the LECCs remain an important law enforcement tool to help the Federal law enforcement agencies and to help focus our Federal resources and lash them up, if you will, with our State and local colleagues and to focus on the particular crime problems in individual districts.

One of the things that the Attorney General has done and the Director has done with respect to our important efforts against terrorism is to again try to use various mechanisms to focus our Federal resources with our State and local colleagues.

For example, in each judicial district there has been established antiterrorism task forces, which are coordinating mechanisms with

respect to the U.S. Attorneys to work with their State and local colleagues to identify particular issues as it relates to terrorist incidents and how to respond to terrorist incidents.

The Director has expanded the FBI's Joint Terrorism Task Forces, which again are investigative bodies but which do take into consideration the use of various State and local resources in this important effort. So I think this kind of approach to Federal law enforcement is important and effective.

Senator SESSIONS. Well, I suppose that we would not dispute that terrorism is the No. 1 priority for the Federal Government at this time, so I don't mean to diminish that. But it may not be the No. 1 priority in a given district, or there may be varied leads, investigations, or activities that need to be undertaken in a given Federal FBI SAC area.

Mr. Mueller, are we sure that we will still be able to give appropriate credit to agents who do important bank robbery cases or important bank fraud cases, or contribute to important drug cases? Are we creating a circumstance in which the FBI is basically saying these are our priorities, you are expected to work these and virtually only these, and the end result would be to pull back from cooperation with local law enforcement in developing the priorities of the district?

Mr. MUELLER. I don't think we can respond in that way. To the extent that an SAC in a particular division has a counterterrorism responsibility—and one of the reasons that we need to give additional resources to the counterterrorism program is you have to develop sources, you have to develop contacts, you have to develop intelligence. And that is often a thankless job in the sense that it does not result in a prosecution that is something you can grasp and take credit for.

So we have to emphasize the counterterrorism program in each of our offices, but I do not want agents sitting on their hands with nothing to do. So what I have asked each of the SACs to do is determine the extent of the workload for agents on the counterterrorism program in their particular division, and then I want to get them that resource, and it may come from other programs.

But with regard to where that SAC takes the manpower from, the SAC should have some say in that because what is good for one SAC in Los Angeles may not be good for the person in Birmingham. The threat in a particular division should be evaluated, and the SAC should have perhaps more flexibility than the SAC has had in the past in devoting those criminal resources to the threat in a particular division once the priority of counterterrorism, counterintelligence, is discharged.

Senator SESSIONS. With regard to setting priorities, which I would indicate to mean if there is a conflict in time, the highest priorities would be served first, I am comfortable with that. I just do not think we should create a circumstance in which we don't have time to do identity theft matters. That is a matter of importance to this committee right now. I believe we are not sufficiently investigating bankruptcy fraud. I think there is a lot of it. It is a Federal court. No one else should do it but the FBI, in my view, and they haven't committed enough there.

So there are some things that I think need to be done. I don't want to see a message go out that so overwhelms the agents that they believe the only thing they can do to gain favor or earn merit is a terrorist or homeland defense-type issue.

Thank you, Mr. Chairman.

Chairman LEAHY. Senator Schumer?

Senator SCHUMER. Thank you, Mr. Chairman.

First, let me thank each of you for your service to our country.

My colleagues have discussed a lot of questions regarding FBI organization, reorganization, efforts after 9/11, and anthrax. I have some followup questions that I would like to put in writing, but I would like to address to Mr. Thompson——

Chairman LEAHY. We will leave the record open for questions in writing from all Senators.

Senator SCHUMER. Thanks, Mr. Chairman.

Now, I would like to ask Mr. Thompson—I just want to take a moment to address with you the extraordinary action taken by the Department yesterday. The Justice Department used footnotes in two Supreme Court briefs to announce a massive change of course in our Nation's gun control policy. For the first time in 60 years, the Federal Government is saying that the right to bear arms is an individual right.

First, this decision wasn't made after discussion, debate, or any open dialog whatsoever. It wasn't made in consultation with Congress or the States, and it wasn't put forward with the kind of detail and analysis that such a significant policy change would usually come with. Instead, it was done undercover, buried in footnotes.

Now, the broad principle that there is an individual right to bear arms is shared by many Americans, including myself, but there are limits on those rights. We limit freedom of speech, the First Amendment, when we say you can't falsely shout "fire" in a crowded movie theater. At the same time, we should be able to put restrictions on who can own guns, and how, when and where they may be possessed.

At his confirmation hearing, Attorney General Ashcroft swore to enforce and defend all existing Federal gun laws. In answer to questions from me, he said, "I understand that being Attorney General means enforcing the laws as they are written, not enforcing my personal preferences."

Then he also said, "I believe that there are constitutional inhibitions on the rights of citizens to bear certain kinds of arms, and some of those I would think good judgment, some of those I would think bad judgment." These are his words. "But as Attorney General, it is not my judgment to make that kind of call. My responsibility is to uphold the acts of the legislative branch of this Government in that arena, and I would do so and continue to do in regard to the cases that now exist and further enactments of Congress."

Well, Mr. Thompson, it just would appear on its face that the Attorney General is doing a 180-degree about-face from what he told us not too long, without any consultation, any notice, any discussion. It is no way to do business and I am sort of shocked by it.

The Department of Justice is saying that the right to bear arms is subject to "reasonable restrictions," but the devil, as always, is

in the details. So I have a series of questions for you about what constitutes a reasonable restriction.

First, is the Federal ban on assault weapons a reasonable restriction? Is the Federal ban on felons owning firearms a reasonable restriction? Has the Justice Department considered how State laws would be impacted?

For example, New York has a strict licensing and registration law. Does the Attorney General's Justice Department believe that the law is unconstitutional? Is Maryland's 7-day waiting period unconstitutional? How about California's ban on Saturday night specials?

The District of Columbia, a city that was not only the Nation's Capital but once it was the Nation's murder capital, has the strictest gun laws in the country. Unless you are law enforcement, you pretty much can't have a gun in D.C. Federal prosecutors enforce D.C.'s gun law. It seems almost by definition, without discussion, that what the Justice Department said in a footnote would overturn that D.C. law.

So I would ask you the answers to these questions. What is the Justice Department's actual view, given that in these two footnotes they reverse 60 years of Government policy, something not reversed by any previous administration, Democrat or Republican? What is the view on these questions?

Mr. THOMPSON. Senator, the footnote that you refer to, as I understand it, was contained in a pleading that was filed by the United States, by the Solicitor General's office, in opposition to a cert petition in which an individual was convicted of a gun crime. That was in the Fifth Circuit. The case was *Emerson*.

Following the *Emerson* decision, the Attorney General sent a memo out to all United States Attorneys in which he committed and set forth his and the Department's view that we are going to aggressively continue to vigorously and aggressively prosecute and enforce the gun laws, and we are going to vigorously defend the gun laws against constitutional attack. He also set forth in that memorandum the position which the court in *Emerson* recognized in its decision, the Fifth Circuit, that the Second Amendment is an individual right.

The footnote was appropriate, in my judgment, as sort of a duty of candor to the Supreme Court to let the Supreme Court know what the Attorney General had communicated pursuant to the Department of Justice——

Senator SCHUMER. So it was a reversal of policy, a dramatic reversal of policy. I mean, there was a 1939 case whose name slips my mind—he will write it down and give it to me—that said, no, the right to bear arms was related directly to the ability of States to raise a militia.

Mr. THOMPSON. I understand that.

Senator SCHUMER. There has been a great deal of discussion about that over the last 62 years about whether that is right or wrong.

Do you disagree that the footnote wasn't a real change in the policy of the United States Government?

Mr. THOMPSON. No, sir. I believe the footnote was appropriate in the context of this litigation, in which the Fifth Circuit embraced

in its decision the Second Amendment individual right to bear arms, and in the context of a duty of candor to the Supreme Court in opposition to this petition.

But to answer your concern, Senator, the Attorney General and the Department are both committed to vigorously enforcing the guns laws and are committed to enforcing those laws against constitutional attack.

Senator SCHUMER. Sir, with all due respect, we don't know what you think the gun laws are. You say you will enforce the law. That is what the Attorney General said at his hearing.

If I might, Mr. Chairman, could I go on a little bit here?

Chairman LEAHY. Yes.

Senator SCHUMER. Yet, they have done what every newspaper today called a dramatic reversal.

Let me ask you this specific question. Would this footnote that there is an individual right to bear arms now mean that there will be a change in policy in regard to the District of Columbia's approach which says unless you are law enforcement, you don't have a right to bear arms?

Mr. THOMPSON. I don't know. I don't want to get too far into discussing the implications of this case because it is pending litigation.

Senator SCHUMER. No, that is not this case. I am asking how you would interpret the new law, the new way the Justice Department reads the Second Amendment in regard to D.C.'s law, not in regard to the *Emerson* case, which is a pretty narrow case.

Mr. THOMPSON. I can only interpret, Senator, how the Justice Department will enforce Federal laws.

Senator SCHUMER. This is Federal.

Mr. THOMPSON. Well, D.C. is a different situation. You are talking about the D.C.

Senator SCHUMER. It is enforcement. It is under the Attorney General's direct supervision.

Mr. THOMPSON. If you are talking about enforcing the gun laws, then as I said before, the Department is going to vigorously enforce the gun laws. In fact, we have an initiative, Project Safe Neighborhoods, in which we are vigorously enforcing crimes committed with guns.

Senator SCHUMER. I understand you are doing certain other things. I would like to get an answer to my specific question, which is will the Justice Department continue to enforce the District of Columbia's gun law which says you can't have a gun unless you are law enforcement? That is basically what it says.

Mr. THOMPSON. As I understand your question, the District of Columbia, while it is controlled by the Congress, is not the type of situation in which I am prepared to answer a question with respect to criminal enforcement. That is what the Attorney General addressed in his memo to all the United States Attorneys.

I don't believe it would have any impact on the District of Columbia. As I understand it, it is a D.C. City Council ordinance.

Senator SCHUMER. But enforced federally, and if you are making a constitutional ruling here or a constitutional assumption that the right to bear arms rests with the individual, it would seem to contradict D.C.'s law.

Mr. THOMPSON. I mentioned to you the Attorney General's memorandum to all the U.S. Attorneys, and as I understand his memorandum, I do not think that the footnote nor his memorandum would change the way we would view the D.C. law that was passed by the D.C. Council.

Senator SCHUMER. The same with New York City's laws, which are not as strong as D.C.'s, but strong, that talk about licensing and registration, fairly strict licensing and registration where you need some rationale to have a gun?

Mr. THOMPSON. Yes, sir.

Senator SCHUMER. And there are no plans afoot to then have another footnote 3 months from now saying that the D.C. law is wrong? Let me ask you one other question. Answer that one and then——

Chairman LEAHY. The Senator's time has expired.

Senator SESSIONS. Well, Mr. Chairman, I would like to clean up after he is through.

Chairman LEAHY. I am going to give the Senator from Alabama the same amount of time as the Senator from New York. As he knows, I always try to balance that out.

We will have time for another round, but Senator Feingold has been waiting for his round. Then it will be my turn next. I will go to the Senator from Alabama and he will be given the same amount of time. I always try to be fair.

Senator SESSIONS. You always do.

Chairman LEAHY. Senator Feingold?

Senator FEINGOLD. Thank you, Mr. Chairman, very much.

For both of you, the Justice Department has consistently refused to provide any information at all on individuals that are being held as material witnesses. The administration has even refused to reveal the number of individuals being held as material witnesses or which courts have issued warrants.

At the same time, I am afraid there are disturbing reports that the authority to detain material witnesses is being abused to lock up individuals who cannot be jailed on other grounds. Press reports have identified more than 20 individuals who may have been jailed on this ground. Again, all of these people are Arabs or Muslims, and some apparently were never even questioned by a grand jury or court before being released. The Washington Post reported earlier this week that one individual was jailed as a material witness after coming forward voluntarily to provide information to the FBI about the hijackers.

A Federal district court in New York last week ruled that the Justice Department used the material witness authority improperly to lock up an innocent individual for almost 3 months in connection not with a criminal trial, but with a grand jury proceeding.

A fundamental constitutional value of this country is that individuals may not be locked up unless they have been accused of or convicted of a crime. A very narrow exception, of course, is provided in the material witness statute, but only under very specific circumstances, and only until the witness' testimony can be preserved for trial.

Given the total secrecy surrounding the Department's use of material witness warrants, and given the news reports that have come

out so far on the Federal court's ruling, how can the American public be reassured that the Government is not simply jailing Arabs and Muslims arbitrarily?

Mr. Thompson?

Mr. THOMPSON. Senator, as a Federal prosecutor and as U.S. Attorney, I in my office routinely used material witness warrants to secure the appearance of a witness before a grand jury. The Department has routinely used these warrants in that way. That is the way, for example, Terry Nichols was detained in connection with the Oklahoma City bombing investigation.

The decision of the judge in the Southern District of New York, to my knowledge, is the first time that the material witness statute was held to be not applicable to a grand jury proceeding. This is an appropriate law enforcement technique in connection with certain kinds of investigations, especially in connection with terrorism investigations, whether they are international terrorist investigations or domestic terrorism investigations, like the Oklahoma City bombing case.

So you have a decision by one judge that, to my knowledge, is counter to how this statute has been interpreted. I would respond to your question by saying that there is nothing inappropriate by the way this statute and this law enforcement technique is being used in these investigations.

Senator FEINGOLD. Mr. Mueller, do you want to respond to that?

Mr. MUELLER. Only to say that whenever one has to get a material witness warrant, one gets the material witness warrant from a judge and you have to make a showing before the judge in order to get the material witness warrant. You have to make a showing to the judge that there is testimony that you want to obtain before the grand jury, and once that testimony has been obtained then ordinarily the person is discharged.

I am not aware of an instance where there is an individual who has been detained for whom we did not want to have information given to the grand jury about certain activities related to terrorism, not just something out of the sky, but related to terrorism. So I think you can assure the American public that this process is monitored by the judiciary and it is engaged in for the purpose of obtaining testimony from individuals who otherwise would not be forthcoming, individuals who do not want to cooperate, but for which we need the use of the grand jury so that they are compelled to testify under oath.

Senator FEINGOLD. Well, I appreciate that answer. I am concerned that there would be abuses in this area, but I certainly will want to follow that up.

Let me ask you another question that is more on the sort of pragmatic side of this. I mentioned earlier the story in the Washington Post on Sunday about an Egyptian immigrant who voluntarily came forward to help the FBI after the September 11 attacks.

Eyad Alrababa went to the FBI because he had some contact with two of the hijackers and thought he could be helpful to the investigation. Instead, he was rewarded with 7 months in Federal custody, almost entirely in solitary confinement, on a material witness warrant, followed by his conviction for a fraud matter unre-

lated to the 9/11 attacks. Eyad, who is engaged to a U.S.-born citizen, now faces deportation once he is released from prison.

Now, in this case and the case involving a Jordanian student, don't you think such use of the material witness statute might discourage people from within the Arab and Muslim community from coming forward with information to help us combat terrorism?

Mr. Thompson?

Mr. THOMPSON. What was the name of the individual again?

Senator FEINGOLD. Eyad Alrababa.

Mr. THOMPSON. I am not familiar with that particular case. But as Director Mueller said, if the material witness warrant was presented to a court with sufficient facts and sufficient predicate activities and necessity pled, then I think the American public could be assured that that was a proper use of the warrant.

I don't think it would necessarily be counterproductive or some kind of negative implication to otherwise law-abiding citizens, whether they be of Arab American background or any other background, from cooperating with law enforcement authorities, Senator.

Senator FEINGOLD. Mr. Mueller?

Mr. MUELLER. I did read the article, and I understand the individual and I think his girlfriend were awfully voluble with the press in terms of their side of the story. I venture to say there is another side of the story in terms of information that was sought by the prosecutors and the investigators. Again, it was a judge supervising this process, and the one item that you did note is that the individual pled guilty to certain offenses at the end of the day.

Senator FEINGOLD. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

As I said, I will skip my time and go to the Senator from Alabama.

Senator SESSIONS. Well, Mr. Chairman, thank you for your courtesy.

With regard to the material witnesses, they can have lawyers, they can write to the newspaper. They are not held so they can't communicate with the outside world. Is that correct?

Mr. THOMPSON. That is correct, Senator.

Senator SESSIONS. All the Department is saying, as I understand it, is they are not going to voluntarily list the names of everybody that is being held, for reasons that the individual may not want their name being out. Maybe their family would be subject to reprisal if they knew that they may be talking to the Government or are being held by the Government. There are a lot of reasons someone might not want their name put in the paper, but they could do so if they wished. Is that not correct?

Mr. THOMPSON. That is correct, Senator. There are legitimate privacy and security concerns with respect to that kind of information being made public.

Senator SESSIONS. I just don't see that we have a problem there. Of course, a judge has to approve the material witness warrant.

Also, under the habeas corpus rule, Mr. Mueller, a defendant can ask to be brought before the judge and require the Government to justify why they continue to hold them. That is the Great Writ that we have in this country. It does apply to these cases, does it not?

Mr. MUELLER. It does, but I have not seen a circumstance where if a material witness, apart from habeas corpus, but a material witness held by a judge where, through the lawyer, there was some reasonable necessity for being brought before the judge, the judge would decline to take that opportunity to find out what the concern was.

Senator SESSIONS. Well, I just think it would cast the wrong impression to suggest that they are held in secrecy, they can't talk to a lawyer, they can't communicate with their family, they can't write a letter out of the prison. Those things are not true. If they want to write the New York Times to say they are being held, they can write them.

With regard to the matter of gun control, this question of whether or not the Second Amendment is a matter of individual rights is a matter, I think, that is important. I think it is a matter of individual rights.

Isn't it true, Mr. Thompson, that Professor Laurence Tribe, the liberal professor, in his constitutional law book, who has studied this issue in depth, has written that it is, in fact, a matter of individual rights?

Mr. THOMPSON. That is my understanding, Senator.

Senator SESSIONS. To say that in a footnote does not mean anything other than that you are candid with the court about what the position of the Department of Justice is with regard to that issue.

Frankly, with regard to the District of Columbia, if their law is so broad that it says only police officers can possess firearms, I hope you will not make a concrete position to suggest you would never question the validity of some of those laws. It may be that on careful review that some of them may not withstand constitutional muster.

We know, of course, that most of the gun control laws have been upheld repeatedly, and I assume the Department is not opposing any of the general laws that we use to enforce against gun violations.

Mr. THOMPSON. I understand that point, Senator, and I would just point out in further response that I think people here, and perhaps even the media, are forgetting that the briefs in question, the briefs that Senator Schumer referred to here—the brief that was filed by the Department of Justice actually defended existing gun laws. It took the position of defending existing gun laws and a conviction. As I said in my response to Senator Schumer, the Attorney General and the Department are committed to a vigorous enforcement of our existing gun laws.

Senator SESSIONS. In fact, do you believe that this Department is enhancing the number of convictions and prosecutions under the existing Federal gun laws?

Mr. THOMPSON. I would hope so.

Senator SESSIONS. The United States Attorney in Alabama told me he was substantially increasing the number of prosecutions in his district for gun violations. I have criticized the former Department of Justice under President Clinton for allowing those prosecutions to plummet by as much as 40 percent. While they wanted to pass laws that bound innocent people, at the same time they were allowing the prosecutions of criminals with guns to go down.

The question of possessing a firearm during commission of a crime, possession after conviction of a felony, filing false documents to obtain a firearm—all the traditional bread-and-butter statutes that we have in law—are not jeopardized by this footnote about individual rights, are they?

Mr. THOMPSON. No, sir.

Senator SESSIONS. Not even close to it?

Mr. THOMPSON. No, sir.

Senator SESSIONS. This Department not only defends those as being legal and constitutional, but is stepping up prosecution of those cases, are you not?

Mr. THOMPSON. That is correct, and in connection especially with our Project Safe Neighborhoods.

Senator SESSIONS. Well, I just think that we need to be more rational here about how we approach this. We have a group that says airplane pilots can't even have a gun in the cockpit in case somebody breaks in and tries to take over the airplane. If they are trained properly, I am amazed that people would object to that.

I think the chairman is concerned, as I am, that a law officer who might cross a jurisdictional line could be arrested because he is carrying a gun that he carries every day of his life in his work.

So I just think it is important for us to know that this is not an action in this footnote that would in any way undermine the commitment of this Department of Justice to not only continue enforcement, but to enhance the enforcement of gun laws. Would you agree with that?

Mr. THOMPSON. That is correct, Senator. I would agree.

Senator SESSIONS. Thank you, Mr. Chairman.

Chairman LEAHY. Just think how easy it would be if all States had Vermont's gun laws. Just so you understand what that means, we have very limited ones. Anyone can carry a loaded concealed weapon in Vermont. There is no permit required. We would even allow you to.

Senator SESSIONS. Even a United States Senator from Alabama?

Chairman LEAHY. From Alabama.

There are two specific things. During deer season, you are limited to the number of rounds you can have in your semi-automatic assault weapon to give the deer a chance. This is true. I mean, this is actually what the law is. Signs go up on the outskirts of Montpelier, our State capital, which notify that during deer season, if you are hunting inside the city of Montpelier, like on the State House lawn, you can only use buckshot. I do not want to start a sudden sweep to Vermont, but that is the law.

This does create a problem, however, and that is during deer season so many out-of-state tourists stop to photograph those signs, usually with the State Capitol prominently in the background, that we have had a number of fender-benders, but the law will probably stay the same.

As I read the opinion we discussed, incidentally, the judge's opinion just recently discussed, the person in New York was held, one, in solitary. Two, he was shipped across the country. And, third, his own lawyer couldn't find him for some time. That makes it a little bit more difficult to file habeas corpus. Most people wouldn't know

how to file habeas corpus. Their lawyer might, but the lawyer has got to find them first.

Gentlemen, we are about to have a vote on the floor on a matter not too far down the coastal highway with Vermont, a matter that we have some interest in, the farm bill. So I will submit the rest of my questions for the record.

I do want to say I appreciate very much your being here. General Thompson, you have had to take on extra duties and I appreciate the way you have taken them on.

Director Mueller, I just want to state for the record that I have called you on a number of very difficult issues, some where I have had questions and members of this committee have had questions, and your candor is most appreciated. I think the kind of candor and directness you have shown is going to serve the Bureau well. There are many who want that.

You have a national treasure in the men and women who work there, and the training they undergo and the standards they have to uphold. We want to make sure that that doesn't get submerged in bureaucracy, but is encouraged to do the best for this country in a very dangerous time. So I appreciate that.

We will stand adjourned.

[Whereupon, at 4:11 p.m., the committee was adjourned.]

[Questions and answers and submissions for the record follow.]

[Additional material is being retained in the Committee files.]

QUESTIONS AND ANSWERS

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. Patrick

DEC 2

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find a response to your written question submitted to the Deputy Attorney General at the hearing before the Senate Judiciary Committee on May 8, 2002. We are providing a response to question 19 relating to the changes section 215 of the USA PATRIOT Act made to provisions of the Foreign Intelligence Surveillance Act (FISA). The Department is continuing to gather information to answer the remaining questions posed to the Deputy Attorney General and the Director of the Federal Bureau of Investigation, and we will forward those responses as soon as possible.

Please note that the response to question 19 requires the Department to provide information that is classified at the SECRET level. That classified information is being delivered to the Committee under separate cover and in accordance with the longstanding Executive branch practices on the sharing of operational intelligence information with Congress.

We appreciate your oversight interest in the Department's activities pursuant to the USA PATRIOT Act. We look forward to continuing to work with the Committee as the Department implements these important new tools for law enforcement in the fight against terrorism. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosure

cc: The Honorable Orrin G. Hatch
Ranking Minority Member

Questions Submitted by Chairman Leahy
Senate Judiciary Committee Hearing on
May 8, 2002

Questions for Director Mueller and Deputy Attorney General Thompson

19. Section 215 of the Patriot Act allows all FBI Special Agents in Charge to obtain court orders requiring the production of "any tangible things (including books, records, papers, documents, and other items)" in connection with terrorism investigations. There have been reports that this authority is being used to obtain records, without showing probable cause that a crime has been committed, from a library or bookstore about what books a person has signed out or purchased.

(a) Has the FBI, in fact, requested such records in any investigation of terrorism?

Answer: Section 215 amended the business records authority found in Title V of the Foreign Intelligence Surveillance Act (FISA). Under the old language, the FISA Court would issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. The USA PATRIOT Act changed the standard to simple relevance and gives the FISA Court the authority to compel production in relation to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

The classified semi-annual report discussing the use of sections 1861-1863 of FISA for the period June 30, 2001 through December 31, 2001 was provided to the Intelligence and Judiciary committees of both houses of Congress on April 29, 2002. That report was provided under cover letter to each committee chairman. Although not specified in the statute, the Department's practice has been to submit the reports covering January1 through June 30 of a given year, by the end of December of that year. The Department of Justice is currently preparing the semi-annual report covering the period January 1, 2002 through June 30, 2002.

The Department is able at this time to provide information pertaining to the implementation of section 215 of the USA PATRIOT Act from January 1, 2002 to the present (December 23, 2002). That information is classified at the SECRET level and, accordingly, is being delivered to the Committee under separate cover.

(b) Can such an order be served on a public library to require the library to produce records about where a library patron has surfed on the Internet? Has such an order been sought by the Department or the FBI?

Answer: Such an order could conceivably be served on a public library although it is

unlikely that public libraries maintain those types of records. If the FBI were authorized to obtain the information the more appropriate tool for requesting electronic communication transactional records would be a National Security Letter (NSL). NSLs can be served on Internet Service Providers to obtain information such as subscriber name, screen name or other on-line names, records identifying addresses of electronic mail sent to and from the account, records relating to merchandise orders/shipping information, and so on but not including message content and/or subject fields.

(c) Do you think that library and bookstore patrons have a "reasonable expectation of privacy" in the titles of the books they have purchased from a bookstore or borrowed from a library?

Answer: Any right of privacy possessed by library and bookstore patrons in such information is necessarily and inherently limited since, by the nature of these transactions, the patron is reposing that information in the library or bookstore and assumes the risk that the entity may disclose it to another. Whatever privacy interests a patron may have are outweighed by the Government's interest in obtaining the information in cases where the FBI can show the patron's relevance to an authorized full investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 11, 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Please find enclosed answers to questions submitted to Deputy Attorney General Larry Thompson, after his appearance before the Committee on May 8, 2002 in the hearing entitled, "Reforming the FBI in the 21st Century: Reorganizing and Refocusing the Mission." We apologize for any inconvenience our delay in responding may have caused you.

We appreciate the additional time provided to the Department to submit responses to the Committee's questions. Our responses to the four remaining questions posed by Senator Leahy (Questions number 1, 2, 14 and 17) will be transmitted to the Committee as soon as possible. In addition, the Department will be transmitting questions posed to Federal Bureau of Investigation Director Robert Mueller, who also testified at the May 8th hearing, shortly.

Thank you for this opportunity to provide additional information to the Committee. If we can be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Jamie E. Brown

Jamie E. Brown
Acting Assistant Attorney General

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Enclosure

Questions Submitted by Senator Leahy for
Deputy Attorney General Thompson
Senate Judiciary Committee Hearing on
May 8, 2002

Leahy 3. **Last year the Justice Department announced that it was reviewing the Attorney General's guidelines for FBI investigations to determine whether changes were needed to deal with the terrorist threat. There are reports, for example, that the guidelines for handling informants are being revised.**

a. **Is the Justice Department considering any changes in the Attorney General's guidelines for investigations or investigative techniques by the FBI or other components of the Department?**

b. **Will Judiciary Committee Members have an opportunity to comment on any changes that are seriously considered?**

Answer: Following the September 11 terrorist attack, the Attorney General ordered a general review of the Department's existing guidelines and procedures relating to national security and criminal matters. The Department's objectives in reviewing the Guidelines was to ensure that the FBI was adequately equipped to protect the public from the continuing threat of terrorism and to reaffirm the Department's commitment to safeguarding the civil liberties and privacy of law-abiding citizens. The review resulted in changes in the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations; the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations; the Attorney General's Guidelines Regarding the Use of Confidential Informants; and the Procedures for Lawful, Warrantless Monitoring of Verbal Communications. The revised guidelines were issued on May 30, 2002. They may be found on-line at www.usdoj.gov/olp/.

Leahy 4. ***No Question Submitted.***

Leahy 5. **On April 11th, the Attorney General directed the Assistant Attorney General for Legal Policy, in consultation with the Criminal Division, to draft procedures to implement the provisions for sharing foreign intelligence information from criminal investigations under Sections 203 and 905 of the USA PATRIOT Act. With respect to those procedures:**

a. **What is the timetable for their completion?**

Answer: The Attorney General adopted guidelines implementing Sections 203, 905(a), and 905(b) on September 23, 2002. They may be found on-line at www.usdoj.gov/olp/.

b. Will Judiciary Committee Members have an opportunity to comment on them before they are adopted?

Answer: Committee staff were provided with copies of the guidelines prior to their release on September 23, 2002, and subsequently were briefed by officials from the Department of Justice, including the FBI, and the Central Intelligence Agency.

c. Will the procedures allow any sharing of "foreign intelligence" information about *lawful* activities of United States persons, including lawful international, commercial or political activities, that is acquired incidentally in criminal investigations?

Answer: Section 905(a) of the USA PATRIOT Act requires law enforcement agencies to share with the Director of Central Intelligence all "foreign intelligence acquired . . . in the course of a criminal investigation." The term "foreign intelligence" is defined in section 3 of the National Security Act of 1947 (50 U.S.C. § 401a) as: "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." In addition, pursuant to section 203 of the USA PATRIOT Act, the Attorney General established procedures for the disclosure of information that identifies a United States person. These procedures provide important safeguards to U.S. citizens identified in information disclosed under section 203 and 905(a) by requiring that all information identifying a U.S. person be labeled by law enforcement agents before disclosure to intelligence agencies. Moreover, upon receipt of information from law enforcement that identifies a U.S. person, intelligence agencies must handle that information pursuant to specific protocols designed to prevent inappropriate use of the information; these protocols were established pursuant to Executive Order 12333, adopted in 1982.

Leahy 6. The FBI has to better focus its missions on the things for which we rely on it in order to address the challenges for the future. With that in mind, in which areas do you think that the FBI should be less involved than it currently is?

Answer: Even before the September 11th attacks, it was evident that the FBI needed to realign its mission priorities, given the various additional investigational responsibilities added to the Bureau's jurisdiction over the last several years. Under the leadership of Attorney General Ashcroft and Director Mueller, the FBI has been making great strides in recalibrating the Bureau's priorities so as to properly balance its core missions – protecting and defending the United States against terrorism and foreign intelligence threats, and upholding and enforcing the federal criminal laws.

Director Mueller has previously testified before this Committee regarding his plans to shift more than 500 field agents from criminal investigations to counterterrorism investigations and other counterterrorism activities. As the Director noted, the overwhelming majority of these agents will be taken from FBI drug investigations, with some additional shifting of agents

currently working on white-collar and violent crimes.

It should be emphasized, however, that the FBI will not abandon its role in combating the drug trade. To the contrary, the Bureau will continue to be an active participant in Organized Crime Drug Enforcement Task Forces with other federal, state, and municipal law enforcement. Even after moving approximately 400 agents from drug-related cases to counterterrorism, the FBI will still devote nearly 1000 agents to drug investigations.

The FBI will also continue to devote high priority to such matters as corporate fraud, civil rights, organized criminal activity, and public corruption. In other areas – such as bank robberies and violent crime – the FBI will look to state and local law enforcement agencies to assume greater responsibility where they have the appropriate expertise and resources. Similarly, as Director Mueller has testified, the Bureau should defer certain cases to agency inspectors general who have the necessary expertise to handle criminal investigations.

Leahy 7. **There are some areas of law enforcement that are uniquely federal. By that I do not mean that there is no role for state and local law enforcement, but that because of the nature of the cases and the challenges they present, that a leadership role by federal law enforcement is required. Terrorism is one such area. I believe that civil rights, complex white collar cases like the tax matters and the Enron, and environmental enforcement are others. Do you share my view that these specific areas – terrorism, civil rights, complex tax or fraud cases, and environmental enforcement are areas in which the federal government needs to maintain a leadership role? If so, why is it that, with the exception of terrorism, the President's proposed budget called for either cuts or flat funding in each of these important areas?**

Answer: We agree that there are areas of law enforcement that are either uniquely federal or that require a federal leadership role. We also agree that the areas you mention – particularly terrorism, civil rights, and complex white collar crime cases -- exemplify law enforcement problems for which the Federal Government must continue to assert primary responsibility.

Leadership is exemplified in many ways that do not necessarily depend upon annual budget increases. The Department has a considerable ongoing base budget. In FY 2002, our appropriation excluding emergency supplemental funding, is $26.7 billion. In FY 2002, we have almost 8,400 authorized attorney positions in our litigating divisions and the United States Attorneys. These resources allow us to respond to many significant cases, like Enron, as they arise without seeking specific additional appropriations. As new priorities arise, resources are shifted to meet our highest priorities. Leadership isn't always about asking for more money, but making wise use of the considerable funds already available from Congress.

Seldom has the Department of Justice asked for resources related to a specific case, because we have base funding to address significant matters. However, the FY 2003 budget

request does include resources in our Civil Division for two high-stakes cases, the Cobell and Tobacco lawsuits, because of the large resource demands they place on the Department.

Like other agencies, the Department must prioritize its budget requests. DOJ has received increases from Congress in recent years for many of our federal responsibilities with workload demands that are, for us, uncontrollable. Examples are housing federal prisoners and detainees, and enforcing immigration laws. Other areas you cite as uniquely federal have also had budget increases, such as counterterrorism and civil rights enforcement. The Administration, and Congress, have targeted resources to programs with particular pressures that demanded additional resources.

The Attorney General has made it very clear that our number one priority is counterterrorism and this Department will do everything within its power to make available the resources necessary to carry out our counterterrorism responsibilities. This does not mean that we will cease our investigative and prosecutorial efforts in other areas where DOJ must take a leadership role. We also look internally in the first instance for resources to satisfy our components' immediate funding requirements, rather than immediately seeking enhancements from the Congress for items that we consider to be high priorities.

Furthermore, we use the authority given to us by Congress to shift resources among components if necessary in order to satisfy unforeseen needs. For example, DOJ may transfer up to five percent of the resources in one appropriation to another. DOJ also has the authority to collect into and redirect annual unobligated balances from our Working Capital Fund. When available, Asset Forfeiture Fund/Super Surplus funding also can be used to cover unforeseen requirements. We notify Congress of our intentions (as required by section 605 of the Department of Justice of Justice Appropriations Act, 2002, P.L. 107-77), but we do not ask for additional resources for every pressing requirement.

We take seriously our leadership role in the law enforcement community, especially for those functions which are inherently federal in nature. We also take seriously our responsibility to be good stewards of the public fisc. The ultimate expression of DOJ leadership is our successful integration and execution of these two critical functions.

Leahy 8. **As a former local prosecutor one thing that used to be very frustrating to me was the law enforcement obsession with "stats." While statistics are an important measurement tool, I have also found that sometimes it leads individual agents or even whole agencies to focus too much on the quantity of cases as opposed to the quality of cases. That is why one provision of S. 1974, for which Senator Grassley has provided important leadership, asks for a GAO report on the collection and use of such statistics by federal agencies. Based on your experience, do you agree that this is a serious problem and, if so, what is being done to try to correct it?**

Answer: While statistical data are often useful, they do not unduly influence the policies and programs of the Department of Justice. As the Attorney General mentioned in November 2001, improving the Department's performance measures so that they are realistic and meaningful, is one of our top management priorities. Under the leadership of the Department's Strategic Management Council, we have established performance goals and indicators that more appropriately reflect outcomes and results. For example, we focus law enforcement efforts on disrupting and dismantling targeted criminal groups, such as major drug trafficking organizations, Asian and Eurasian criminal enterprises, and major violent gangs. Inherent in the shift to focusing on results is also a shift in the nature of investigations that will ultimately lead to those results–more investigations is not necessarily better. We do, however, keep data on key operational steps in the process to be able to assess the resources we have used to achieve our results, and to estimate future resource needs.

Measuring law enforcement performance presents unique challenges. "Success" for the Department of Justice is achieved when justice is served fairly and impartially. It cannot be reduced to simple numerical measures of arrests, indictments, or convictions. Therefore, although the Department accumulates actual data on a select number of these activities, it does not target numerical levels of performance.

Leahy 9. **The Department of Justice is divided between political appointees and career prosecutors and attorneys. The American people depend on these hard working career public servants for consistency in enforcement and to bolster public confidence that federal cases are being brought or not brought based on the law and the evidence, and not on politics of either party that controls the executive branch. According to media reports, there have been a series of SES-level career officials and section chiefs at the Department of Justice who have been replaced since the new Administration assumed power. These include the head of the Public Integrity Section in the Criminal Division, the Chief of the Employment Section in the Civil Rights Division, the head of the Federal Programs Branch in the Civil Division, and more. Some of these people have been at the Department for decades through previous administrations from both parties, and some of their replacements – at first glance – do not appear to have the same level of legal experience. While I am not asking about these cases individually, would you agree with the general proposition that career prosecutors and Department lawyers should not be removed from their positions because of their political views and that career SES positions should not be filled based on a person's political affiliations but based on their legal experience.**

Answer: The Department of Justice strives to fill all of its legal positions with the most, talented, qualified and experienced attorneys. It is not the Department's policy to inquire into the political views or affiliations of career Department attorneys (or candidates for career attorney positions), or to base any personnel actions on the political views or affiliations of career

attorneys, to the extent that such views are known.

Leahy 10. **The Defense Department has announced a plan which creates a new four-star command, U.S. Northern Command, with the mission of "defending the United States and supporting the full range of military assistance to civil authorities." A Defense Department official stated that the commander would look at what legal restrictions may have to altered. The Judiciary Committee, along with the Justice Department, needs to ensure that this new command does not "creep" into areas that are within the proper purview of civil authorities. What was the Justice Department's input into the decision to establish Northern Command?**

Answer: The Department of Defense's decision to create the U.S. Northern Command was made in the context of its own assessment of the mission needs of the Department of Defense during its revision of the Unified Command Plan. Because the Unified Command Plan relates to internal DoD organization and assignment of responsibilities, the Department of Justice was not consulted on this plan.

Leahy 11. **What is the Justice Department's role in monitoring or participating in domestic activity by the military, and are there any areas of military support to civil authorities that the Department does not currently monitor or participate in?**

Answer: If circumstances occurred where it became necessary for military units to act in support of US law enforcement, such activities would occur pursuant to established guidelines, depending on the nature of the activity DoD sought to undertake. Those guidelines, including rules on the use of force, are coordinated with the Department of Justice. Certain DoD activities entail more Department of Justice involvement than others. For example, DoD's Counterintelligence Field Activity/Joint Counterintelligence Assessment Group participates in and currently provides significant logistic and technical support to the Foreign Terrorist Tracking Task Force. In addition, DoD's participation in missions to quell civil disturbances under the Insurrection Statutes, if necessary, would be undertaken at the direction of the President, generally at the request of, or on the advice of, the Attorney General. Additionally, DoD activities in support of federal efforts to counter terrorist incidents involving weapons of mass destruction would be undertaken at the request of the Attorney General. On the other hand, military activities in support of state and federal law enforcement agencies in the counternarcotics arena are coordinated by such agencies and would not necessarily be monitored by the Department of Justice.

Leahy 12. **When Robert Hanssen pled guilty to espionage, he agreed to cooperate with the government's damage assessment. A sentencing memorandum indicates disagreement in the Justice Department and the Intelligence Community over whether Hanssen has cooperated fully in his debriefings. Please provide**

a copy of this memorandum and explain how the decision was made to recommend to the judge that the plea agreement should stand.

Answer: In response to your request we have provided you with the attached sentencing memorandum. As the memorandum makes clear, the prosecutors in this case were provided with differing assessments by components of the intelligence community and the Department of Justice about the extent to which Hanssen complied with his cooperation agreement. In the face of divergent views, the Department considered whether it had sufficient grounds to move the court to abrogate the plea agreement. After careful study of this issue, which included a request for and the review of additional facts and justification from several of the components which debriefed Hanssen, the Department concluded, at the very highest levels, that it could not carry its burden of establishing that Hanssen breached his agreement. The Department recognized, as well, that even if it were able to meet this burden, it would still have to consider, weigh and evaluate the burden on national security which would result from proceeding to trial.

Leahy 13. **In response to a question from Senator Cantwell and me, the FBI advised the Committee on May 2nd that the Justice Department recently issued "Procedures for the Use of Classified Investigative Technologies in Criminal Cases." Please provide a copy to the Committee and explain what factors will be considered in deciding whether to approve the use of classified technology, such as sophisticated surveillance methods used against FISA targets, in a criminal investigation.**

Answer: Please see the attached memorandum of January 31, 2002, from Deputy Attorney General Thompson on "Procedures for the Use of Classified Investigative Technologies in Criminal Cases".

Leahy 15. **I would like your reaction, as a former U.S. Attorney to reports we are hearing that some U.S. Attorneys feel there is a new trend to centralize control over criminal cases, including terrorism cases, at the Department. For instance, we have heard that local FBI field offices have been directed in some cases not to share information directly with the federal prosecutor down the street from them, but instead to send it to Washington first, and let Washington send it back to the U.S. Attorney. Is that happening? Has the Department reevaluated the relationship between the U.S. Attorneys in each District and the Criminal Division and, based on your past experience, do you think that is wise?**

Answer: We are unaware of any new trend or directive to centralize control over all criminal cases at the Department in Washington. To our knowledge, FBI field offices have never been restricted in the sharing of information in criminal cases with U.S. Attorneys' Offices.

However, there are certain types of investigations with national security implications that

for many years have been subject to greater scrutiny and control from Washington. For example, many foreign intelligence and foreign counterintelligence investigations employ investigative methods pursuant to the Foreign Intelligence Surveillance Act (FISA). The acquisition, retention, and dissemination of FISA information is governed by the statute's minimization provisions, which require the Attorney General to propose, and the Foreign Intelligence Surveillance Court (FISC) to approve, minimization procedures in each case. See 50 U.S.C. 1801(h), 1821(4). Moreover, the disclosure for law enforcement purposes of information acquired pursuant to FISA is governed by other provisions of the statute. 50 U.S.C. 1806(b), 1825(c). The Department of Justice's March 6, 2002, Intelligence Sharing Procedures, a copy of which was previously provided to the Committee, provide in pertinent part that in "investigations involving international terrorism, the relevant [U.S. Attorneys' Offices] shall receive information and engage in consultations to the same extent as the Criminal Division." As the Committee is aware, the March 6, 2002, Procedures were approved by the Foreign Intelligence Surveillance Court of Review. See In re Sealed Case, 310 F.3d 717 (2002).

National security and terrorism cases are among the most sensitive cases handled by the Department and they require a consistent and coordinated enforcement program nationwide. Accordingly, the bringing of espionage cases is closely controlled by the Criminal Division. Similarly, the U.S. Attorneys Manual has long required consultation and approval of the Criminal Division prior to the initiation of terrorism investigations and prosecutions. By statute, some terrorism charges require certification by the Attorney General before they can be brought. Moreover, under 50 U.S.C. 1806(b) and 1825(c), "[n]o information acquired pursuant to [FISA] may be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General." Thus Washington plays a significant role in these cases.

Nevertheless, the Attorney General's initiative to designate Anti-Terrorism Coordinators (ATCs) and to establish Anti-Terrorism Task Forces in each U.S. Attorney's Office indicates that more responsibility for developing terrorism cases is, in fact, being afforded to U.S. Attorneys. The Department is currently involved in a comprehensive effort to provide training for all ATCs to better enable them to handle their expanded responsibilities in the terrorism area.

Leahy 16. You testified that the Strategic Management Council's review of the FBI will consider the Inspector General's report on the FBI's handling of the Hanssen espionage case and that you anticipate receiving the IG's report "in the next few months." Does this mean that the Council will not make its recommendations to the Attorney General until then -- as late as next fall -- and that you have not yet identified any substantive FBI management issues that can be shared with the American people at this stage?

Answer: The Strategic Management Council (SMC) is in the process of completing its report while endeavoring to take account of recent developments. Completion of the report is not tied

to the IG's completion of his report in the Hanssen investigation.

Questions Submitted by Senator Feingold for
Deputy Attorney General Larry Thompson
Senate Judiciary Committee Hearing on
May 8, 2002

Feingold 8. On October 31, 2001, the Attorney General said:

"Aggressive detention of lawbreakers and material witnesses is vital to preventing, disrupting, or delaying new attacks. It is difficult for a person in jail or under detention to murder innocent people or to aid or abet in terrorism."
(Speech of Attorney General Ashcroft, Outlines Foreign Terrorist Tracking Task Force, October 31, 2001, U.S. Dept. of Justice; see also United States v. Awadallah, No. 01-Cr-1026, slip op. at n.28 (S.D.N.Y. Apr. 30, 2002).)

But, in ruling that Mr. Osama Awadallah was illegally arrested on a material witness warrant, the federal district court in New York recently found that "[r]elying on the material witness statute to detain people who are presumed innocent under our Constitution in order to prevent potential crimes is an illegitimate use of the statute." (slip op. at n. 28.)

Does the Department of Justice still believe that individuals can be detained under the material witness statute to prevent them from engaging in criminal activity?

Answer: A person may be detained under the material witness statute, 18 U.S.C. § 3144, if a federal judge concludes that (1) his testimony is "material in a criminal proceeding," (2) it may become impracticable to secure his presence by subpoena, and (3) he meets the criteria for detention under the Bail Reform Act, 18 U.S.C. § 3142. Generally, once the witness gives full and complete testimony, he is released unless he is held under some other authority (e.g., immigration detainer, detention on pending charges). The Department has historically taken the view that Section 3144 applies in the grand jury context, and it has used Section 3144 to detain material grand jury witnesses for many years. Terry Nichols, who was detained on a material witness warrant before the Oklahoma City indictment was returned, is a prominent example of that use. The Department's position is consistent with the only applicable appellate precedent directly on point, Bacon v. United States, 449 F.2d 933 (9th Cir. 1971), and the views of Congress when the material witness statute was re-codified in 1984, see S. Rep. No. 98-225, at 28 n.88 (1983), reprinted in 1984 U.S.C.C.A.N. 3182, 3211. We therefore disagree with the decision in United States v. Awadallah, 202 F. Supp. 2d 55 (S.D.N.Y. 2002), which is currently on appeal to the Second Circuit. We also note that, after the decision in Awadallah, the Chief Judge of the Southern District of New York issued a contrary decision that was strongly critical of the reasoning in Awadallah. See In re Application of U.S. for a Material Witness Warrant, 213 F.

Supp. 2d 287 (S.D.N.Y. 2002).

Feingold 9. You testified at the hearing that use of material witness warrants is "an appropriate law enforcement technique in connection with certain kinds of investigations, especially in connection with terrorism investigations." Does the Department use the material witness statute differently in the context of terrorism investigations than in the context of other criminal investigations? If so, how?

Answer: The Department does not use the material witness statute differently in the context of terrorism investigations than in the context of other investigations. For example, it routinely uses Section 3144 to detain foreign nationals who may have information relating to a smuggling offense and who, in the absence of detention, are unlikely to remain within the United States where they will be subject to subpoena.

Feingold 10. Were the policy decisions about the use of the material witness authority in connection with the September 11th investigation made by the Department headquarters? What kind of directives or guidance were provided to the U.S. Attorney's Office in New York and other U.S. Attorney Offices in connection with material witnesses and the September 11th investigation?

Answer: The policy decisions were made at the Department of Justice in consultation with the U.S. Attorneys' Offices and there have been continuing contacts to communicate those decisions.

Feingold 11. How many individuals arrested on material witness warrants in connection with the September 11th investigation were held in high security facilities? How many were held in the high security part of the Metropolitan Corrections Center in New York where Mr. Awadallah was held?

Answer: Information about material witness warrants pertains to matters occurring before a grand jury, which we are prohibited from disclosing by Federal Rule of Criminal Procedure 6(e). We can advise, however, that all such persons, who were found by federal judges to have information material to the grand jury's investigation, were held in accordance with security precautions that were intended to ensure the safety of the institutions in which they were housed, the personnel and other inmates at the facilities, and the witnesses themselves.

Feingold 12. How many individuals who were arrested as material witnesses in connection with that investigation have since been released? Of those, how many testified before a grand jury before being released?

Answer: As noted above, we are prohibited by Rule 6(e) from disclosing this information.

Feingold 13. How many individuals are currently in custody on material witness warrants in connection with the terrorism investigation? Of those, how many are being held as grand jury witnesses? And when do you expect that their testimony will be presented to a grand jury?

Answer: We are prohibited by Rule 6(e) from disclosing this information.

Feingold 14. At least two individuals who were arrested on material witness warrants were subsequently charged with lying: Mr. Awadallah, whose indictment for perjury before the grand jury has now been dismissed; and Mr. Higazy, whose indictment for lying to federal agents was voluntarily dismissed by the government when they were finally convinced that he was telling the truth.

(a) How many individuals first arrested on material witness warrants were subsequently charged with lying or perjury or similar crimes for statements made after their arrest?

Answer: Two individuals first arrested on material witness warrants were subsequently charged with making false declarations or perjury.

(b) How many individuals first arrested on material witness warrants were subsequently charged with any other crime?

Answer: We are prohibited by Rule 6(e) from disclosing this information.

Feingold 15. How many individuals arrested on material witness warrants were provided with a lawyer at government expense to appear at a bail hearing?

Answer: Counsel is provided for all "financially eligible" material witnesses arrested under 18 U.S.C. § 3144. See 18 U.S.C. § 3006A(a)(1)(G). ("[r]epresentation shall be provided for any financially eligible person who * * * is in custody as a material witness").

Feingold 16. The opinion in the Awadallah case outlines in detail the warrant proceedings before the magistrate who issued the arrest warrant. How many such hearings for material witnesses were sealed at the time they were held? What was the duration of each of those sealing orders? Have any of those sealing orders since been lifted?

Answer: If an individual is a witness in a grand jury proceeding, the material witness warrant and all proceedings relating to the witness will be sealed in accordance with the grand jury secrecy rule, Fed. R. Crim. P. 6(e)(2) & (6) ("Records, orders, and subpoenas relating to grand jury proceedings shall be kept under seal to the extent and for such time as is necessary to prevent disclosure of matters occurring before a grand jury."). Generally, these materials remain

sealed unless or until they have been made public in a criminal trial or other judicial proceeding.

Feingold 17. The federal court in New York outlines actions by federal agents that it finds to be illegally coercive seizures of Mr. Awadallah in violation of the Fourth Amendment. How many of the individuals detained as material witnesses were told by federal agents or lawyers that they faced criminal or immigration charges?

Answer: As stated in the response to question 14, above, we are prohibited from disclosing this information per Rule 6(e).

Feingold 18. What is the race, ethnicity, citizenship, national origin, and religion of each of the individuals detained as material witnesses?

Answer: As stated in the response to question 14, above, we are prohibited from disclosing this information per Rule 6(e).

Questions for Director Mueller and Deputy Attorney General Thompson

Feingold 19. Section 215 of the Patriot Act allows all FBI Special Agents in Charge to obtain court orders requiring the production of "any tangible things (including books, records, papers, documents, and other items)" in connection with terrorism investigations. There have been reports that this authority is being used to obtain records, without showing probable cause that a crime has been committed, from a library or bookstore about what books a person has signed out or purchased.

(a) Has the FBI, in fact, requested such records in any investigation of terrorism?

(b) Can such an order be served on a public library to require the library to produce records about where a library patron has surfed on the Internet? Has such an order been sought by the Department or the FBI?

(c) Do you think that library and bookstore patrons have a "reasonable expectation of privacy" in the titles of the books they have purchased from a bookstore or borrowed from a library?

Answer: *Sent to the Committee in a December 23, 2002 letter from Assistant Attorney General Daniel J. Bryant.*

Feingold 20. Section 215 also includes a provision that prohibits anyone who receives an order to produce business records from disclosing that fact to any person.

Does the Department interpret that provision to prohibit a person receiving an order from communicating with a lawyer about how he or she should respond?

Answer: Section 215(d) provides that "[n]o person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section." We do not interpret this to mean that an individual or a corporation could not discuss the order with their lawyer, at least if such discussion was necessary to produce the tangible things.

Senator Leahy Question #12 Attachment

FILED
6
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 01-188-A
	)	
ROBERT PHILIP HANSSEN,	)	
	)	
Defendant.	)	

SENTENCING MEMORANDUM

Robert Philip Hanssen is a traitor. For all the words that have been written about him, for all the psychological analyses, the speculations about his motivation, and the assessments of his character, this is, at the end of the day, all that really warrants being said about Hanssen. He is a traitor and that singular truth is his legacy.

He betrayed his country – and he did so at a time when we were locked in a bitter and dangerous cold war with the Soviet Union. Hanssen's brazen and reckless misconduct, its surpassing evil, is almost beyond comprehension. Using the very tools he acquired as an FBI counterintelligence expert, he covertly and clandestinely provided the Soviet Union and then the Russians information of incalculable significance, extraordinary breadth, and exceptionally grave sensitivity. He did so knowing that his disclosures could – and ultimately did – get people killed and imprisoned, and he did so knowing that they placed in jeopardy the safety and security of our entire nation.[1] That we did not lose the Cold War ought blind no one to the fact that Robert

[1] All one has to do is look at the descriptions of some of the documents he compromised to the Soviets. See, e.g. Count 8 ("A TOP SECRET United States intelligence analysis of the effectiveness of Soviet intelligence collection efforts against certain United States

Philip Hanssen, for his own selfish and corrupt reasons, placed every American citizen in harm's way.

He betrayed the Federal Bureau of Investigation, not only in the sense that he betrayed its core mission of protecting our national security and our citizenry, but also in the sense that, having taken an oath of office to "support and defend the Constitution of the United States against all enemies, foreign and domestic" and having sworn to "bear true faith and allegiance to the same", he betrayed his thousands of fellow agents and fellow FBI employees who, unlike Hanssen, were truly committed to the core values of Fidelity, Bravery and Integrity.

And he betrayed the American people. Hanssen had an irreducible duty of loyalty to the American people – and not because, or not *just* because, he was a federal law enforcement officer with official responsibility for countering the Soviet and Russian espionage threat. Rather, Hanssen owed the American people his allegiance, his constancy and his faithfulness for no better reason, and there could be no better reason, than that he enjoyed the privilege of American citizenship. Instead, by his treachery, he made this a more dangerous and volatile world in which to raise our families.

Finally, Hanssen undermined the people's confidence in our government's ability and capacity to protect and defend even the FBI, the premier law enforcement agency in the world, from the perfidy of spies. In so doing, he did injury and insult to this American institution, a harm only partially ameliorated by the recognition that it was the FBI, to its enormous credit and

---

nuclear weapons capabilities....") and Count 12 ("A highly-restricted TOP SECRET/SCI analysis, dated May 1987, of the Soviet intelligence threat to a specific and named highly-compartmented United States Government program to ensure the continuity of government in the event of a Soviet nuclear attack....")

honor, that unmasked Hanssen and brought him to justice.

Time is not likely to heal this particular wound. It is as raw, as penetrating, and as grievous today as it was the day Robert Philip Hanssen was arrested. In large part that is a product of the catastrophic impact of Hanssen's misconduct, beginning with the executions of Sergey Motorin and Valeriy Martynov, two KGB officers recruited by the United States intelligence services, compromised by Hanssen, and put to death by the Soviet Union. Even though Aldrich Ames also compromised each of them, and thus shares responsibility for their executions, this in no way mitigates or diminishes the magnitude of Hanssen's crimes. *Their blood is on his hands.*

And that is only the beginning: Hanssen's technical compromises cost the United States not only the value of its investments but the priceless value of lost opportunities to gather intelligence of the most vital importance to the United States. Hanssen's systematic compromise of comprehensive intelligence material concerning past successes and failures, current activities and capacities, and future intelligence plans, could only have left the Soviets and Russians in stunned disbelief that they should be privy to such material. Hanssen's betrayal of other human sources and assets not only compromised their value as reliable sources of intelligence information, but jeopardized their very lives. These individuals sided with America and made the hard and dangerous choice to help our country, not knowing of course that their existence and cooperation would come to be known to an individual who had made a profoundly different choice as to his basic allegiance. Similarly, Hanssen's clandestine warnings to the Soviets and Russians about some of the most sensitive investigative and intelligence collection activities of the United States intelligence community – such as the espionage investigation of Felix Bloch

and ongoing technical operations of extraordinary value and significance – gave the Soviets and Russians the knowledge and ability to frustrate and even thwart essential intelligence activities of the United States Government.

For his betrayal of our country, and for the unpardonable consequences of his misconduct, Hanssen deserves to forfeit his right ever to live again within our community and within our society.[2]

COOPERATION

Before Hanssen pled guilty, he faced a potential death sentence. Specifically, fourteen of the counts in the indictment carried the required statutory language that made them death penalty eligible. As part of the plea, the United States gave up the potential for a death penalty sentence and it did so for two principal reasons. First, a contested trial of this matter would have itself imposed a severe burden on our national security. Second, it was essential to the United States intelligence community that it obtain a thorough and comprehensive debriefing of the defendant and the only way to obtain this was through a Plea Agreement. Indeed, it is a fundamental requirement of the defendant's Plea Agreement that he "cooperate fully, truthfully and completely with the United States...." see Plea Agreement at ¶ 10, the violation of which would constitute a breach of the agreement and subject it to termination[3].

---

[2] The parties agreed and stipulated as part of the Plea Agreement that the appropriate sentence for the defendant was life imprisonment without parole or reductions for good behavior or for any other reason. See ¶ 5 of the Plea Agreement. The Court accepted the Plea Agreement and, pursuant to a Rule 11(e)(3) Order, agreed to embody in its judgment and sentence the agreed upon disposition. See ¶ 6 of the Plea Agreement and the Court's Rule 11(e)(3) Order entered June 14, 2001.

[3] It should be emphasized here that a party claiming a breach of a Plea Agreement has a heavy burden of proof, whether it is a defendant attempting to get out of a deal he regrets or

It is now ten months since the entry of the defendant's guilty plea and, while the defendant's cooperation obligation is "a lifetime commitment", see Plea Agreement at ¶ 10(g), it is appropriate that we assess at this time whether the defendant has honored his cooperation obligation.

Four United States Government entities have debriefed Hanssen: (1) The FBI; (2) The Hanssen Damage Assessment Team ("HDAT"), an interagency task force created at the direction of the Director of Central Intelligence for the purpose of assessing the damage caused by Hanssen; (3) The Commission for the Review of FBI Security Programs (the "Webster Commission"); and (4) the Inspector General of the Department of Justice. Each entity, at the request of the United States Attorney's Office, has written a letter or memorandum to this office summarizing their assessment of Hanssen's cooperation.[4]

At the outset, it should be noted that the defendant submitted to several hundred hours of debriefings and, with the exception of a brief time period after September 11th when FBI personnel were unavailable to conduct debriefings, Hanssen has met with law enforcement and intelligence entities continuously since the entry of his plea. The FBI debriefed Hanssen on 41 separate occasions, including two proffer sessions prior to entry of the plea. The HDAT debriefed Hannsen on 27 separate occasions. Coupled with the interviews done by the Webster

---

the Government asserting that a defendant has not lived up to the terms of his agreement. In either case, the party claiming a breach must prove by a "preponderance of the evidence" that the other party has broken the agreement in a material manner. See United States v. Conner, 930 F.2d 1073, 1076 (4th Cir. 1991). See also ¶32 of the Plea Agreement.

[4] Although several of these documents are excerpted in this memorandum, the full documents contain sensitive and/or classified material and, therefore, are filed with the Court in an in camera and classified submission, along with the results of two polygraph examinations of the defendant.

Commission and the IG, Hanssen submitted to some 75 separate interviews during this ten month period. In addition, he submitted to polygraph examinations conducted by two different entities, underwent psychological evaluations and testing and, at the request of the United States Attorney's Office, waived both an attorney-client privilege and a priest-penitent privilege.

We turn first to the FBI's assessment of Hanssen's cooperation. In the evaluation of a defendant's cooperation, the United States Attorney's Office principally relies upon the investigative agency responsible for the case. In this case, that is the Washington Field Office of the FBI. The FBI's judgment, which was based on some six months of interviews, is that Hanssen was "in substantial compliance with the terms of his plea agreement." Specifically, the FBI notes, Hanssen "provided information during the debriefings that was identical or consistent with independent investigative results, and in some cases was previously unknown to us and damaging to himself."

HDAT and the IG, however, perceived Hanssen's cooperation in essentially negative terms. Both entities expressed to this Office serious reservations about Hanssen's candor and cooperation. The HDAT particularly questioned Hanssen's claims of a poor memory as an excuse for either not engaging fully in the debriefing or as a means to hide facets of his activity. Similarly, the IG found that Hanssen's answers were often contradictory, inconsistent, or illogical, and found Hanssen's cooperation concerning his finances, the significance of his espionage and his motives to be "particularly problematic."

Finally, the Webster Commission concluded that it had no reason to conclude that Hanssen had not responded to its questions fully, truthfully and completely.

Thus, this Office has before it four evaluations, two of which can generally be

characterized as positive and two which can generally be characterized as negative.[5] In light of these assessments, this Office considered whether it had a sufficient basis by which to move this Court to abrogate the Plea Agreement, in other words, whether we have sufficient hard and admissible evidence by which to convince a Court that he has broken his promise of full and candid cooperation. There are three factors that convince us that we could not carry this burden, even if we chose to declare a breach of the agreement:

First, this case does not involve a defendant who refused to be debriefed at all or who cut off debriefings at some point in time; rather, this defendant has submitted to hundreds of hours of debriefing, on some 75 separate occasions, underwent psychological testing and, upon request, executed waivers to permit the Government to seek information which was otherwise privileged.

Second, while we are troubled and concerned with the IG and HDAT reservations about Hanssen's candor, a breach proceeding would require an evidentiary hearing in which the Government would have to prove to the Court's satisfaction, and by a preponderance of the evidence, that the defendant breached his agreement. Typically, that would suggest evidence of either a complete failure to cooperate or the making of false statements of such an explicit and unequivocal nature that it could even subject a defendant to a false statements or perjury prosecution. We do not believe we have that here. Rather, what we have here are conscientious analytical judgments and assessments which have led both HDAT and the IG to have serious reservations about the defendant's candor and cooperation but which do not permit abrogation of the plea agreement. As the HDAT acknowledged in its report: "We recognize that our

---

[5] In addition, this Office also has before it two polygraph summaries, each of which is classified SECRET, and therefore cannot be further described in this pleading. However, both summaries are submitted in camera to the Court.

assessment of Hanssen's cooperation may not give you hard, actionable facts that can withstand legal scrutiny."

Finally, we have before us the considered judgment of the FBI, signed by a senior FBI Headquarters official, and reflecting a conclusion based on approximately six months of comprehensive debriefings, which states that the defendant was in "substantial compliance" with his obligation of full, truthful and complete cooperation.

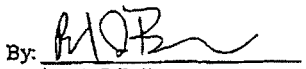
Given these factors, the Government cannot carry its burden of proving a breach of the Plea Agreement. It should be emphasized here that, even if we could carry this burden of proof, that would not be dispositive as to the appropriate course of action. The Government would also have to consider, evaluate and weigh the burden on national security associated with proceeding to trial, a principal concern and consideration in every national security prosecution. In this respect, we would note that Paul J. Redmond, Chief of the Hanssen Damage Assessment Team, has advised the Department of Justice that despite his significant reservations about Hanssen's candor and completeness, on balance he believes it would not be in the national security interest of the United States to abrogate the plea agreement and put Hanssen on trial.

WHEREFORE, we respectfully request that the Court sentence Robert Philip Hanssen to

life in prison.[6]

Respectfully submitted,

PAUL J. McNULTY
UNITED STATES ATTORNEY

By: 

Randy I. Bellows
Justin W. Williams
Gordon D. Kromberg
Assistant United States Attorneys
Laura A. Ingersoll (AUSA/D.C.)
formerly: Senior Trial Attorney, USDOJ

---

[6] ¶ 21 of the Plea Agreement concerns the cooperation of the defendant's wife, Bernadette Hanssen. The paragraph indicates that, if Mrs. Hanssen continues to be fully cooperative, the Government will invoke at the time of sentencing the provisions of 5 U.S.C. § 8318(e) to provide Mrs. Hanssen the equivalent of a survivor's annuity. Prior to sentencing, the Government will advise the Court as to whether Mrs. Hanssen has continued to be fully cooperative. If so, the Government will provide the Court a copy of the certification contemplated by 5 U.S.C. § 8318(e).

CERTIFICATE OF SERVICE

I hereby certify that I have caused the foregoing SENTENCING MEMORANDUM to be served, by first class mail, on:

Law Offices of Plato Cacheris
1100 Conneticut Avenue, N.W.
Suite 730
Washington, D.C. 20036

this 6 day of May, 2002.

Signed: _____
Randy I. Bellows

Senator Leahy Question #13 Attachment

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

January 31, 2002

MEMORANDUM FOR THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
ALL UNITED STATES ATTORNEYS
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINISTRATION
THE COMMISSIONER OF THE IMMIGRATION AND NATURALIZATION SERVICE
THE DIRECTOR OF THE UNITED STATES MARSHALS SERVICE

FROM: Larry D. Thompson
Deputy Attorney General

SUBJECT: Procedures for the Use of Classified Investigative Technologies in Criminal Cases

The widespread availability of new technologies, such as encryption, can present significant problems in searching for and obtaining evidence of crimes. At the same time, technological advances may be available to law enforcement to surmount these problems. However, the use of sophisticated technologies in criminal investigations can raise novel and difficult issues of law and policy, especially where significant law enforcement or national security interests could be implicated by the public disclosure of details relating to those technologies during the course of legal proceedings.

To ensure that the use of such technologies in criminal investigations is approached in a careful and coordinated manner, I am hereby instituting the following measures. The requirements of this memorandum are intended to meet two objectives: first, that we make fully informed decisions about whether and how to use classified investigative technologies in criminal cases; and second, that we draw on the fullest possible range of legal and technical expertise in determining how best to proceed in obtaining evidence in increasingly complex technical settings.

I. Scope of this Memorandum.

(A) "Classified investigative technology". For purposes of this memorandum, the term "classified investigative technology" means any hardware, software, or other investigative technology that satisfies the following criteria:

(1) the hardware, software, or other investigative technology is designed to intercept or acquire information of evidentiary value as a result of a system or process which is based, in whole or in part, upon information which, at the time of its use, has been classified pursuant to Executive Order 12958 of April 17, 1995, as amended, or any successor Executive Order; and

(2) there is a reasonable possibility that–

(a) the evidentiary information to be obtained by the technology will be sought to be introduced into evidence in order to prove any charge brought by the United States;

(b) disclosure of details concerning such technology will be necessary to authenticate evidentiary information sought to be introduced into evidence in order to prove any charge brought by the United States; *or*

(c) the use of the particular technology will be the subject of a motion to suppress or other such litigation.

(B) "Deployment in a criminal investigation". This memorandum applies only to technologies deployed in connection with an authorized criminal investigation. This memorandum does not apply to the deployment of a technology in any collection activity authorized under the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), or Executive Order No. 12333 (United States Intelligence Activities), 46 Fed. R. 59941 (December 4, 1981). The requirements and procedures applicable in such matters remain unaffected by this memorandum.

II. Procedures with Respect to Classified Investigative Technologies.

(A) Prior Approval Required for Deployment of Classified Investigative Technologies in Criminal Investigations. Prior to the deployment of a classified investigative technology in a criminal investigation, the relevant United States Attorney's Offices, as well as any Departmental investigative agency involved, shall promptly notify the Criminal Division of the proposed deployment. Thus, for example, the Federal Bureau of Investigation, the Drug Enforcement Administration, the Immigration and Naturalization Service, and the United States Marshals Service must bring any proposed deployment of a classified investigative technology in a criminal investigation to the attention of the Criminal Division. To the extent that an investigative agency has not already done so, it shall at the same time also notify the relevant United States Attorney's Offices of any such proposed deployment.

Upon such notification, the Assistant Attorney General for the Criminal Division (AAG) shall ensure that the Criminal Division promptly and fully consults with the relevant investigative agency involved, and (in any case in which the technology in question is one

developed in whole or in part by the Federal Bureau of Investigation) with the FBI. The AAG shall thereafter make a recommendation regarding the contemplated deployment, taking into account the nature of the investigation, the nature of the evidence to be obtained, the type of judicial or other authorization required to obtain the evidence, the risk of public disclosure of the method during the course of litigation, the law enforcement or national security interests that could be implicated by disclosure of the method, the privacy interests at stake, and the availability of court-ordered protective measures. The recommendation shall promptly be forwarded to the Deputy Attorney General for review and approval or disapproval of the recommendation.

In reviewing a proposed deployment, the Criminal Division should consider the extent to which different forms of judicial orders could affect the risk that a classified investigative technology will later be ordered to be disclosed. For example, it is important to recognize that the use of novel methods in the course of an interception or seizure of computer data can present significant questions about the appropriate form of judicial order to be sought in a particular case. Highly technical considerations, with respect both to configuration of the object of the order and to the investigative method to be used, may, for example, dictate whether a search warrant or Title III order is appropriate. Thus, part of the Criminal Division's role in reviewing the use of classified investigative technologies will be to draw on available technical expertise, as needed, in the consideration of legal and policy issues.

(B) Prompt Notification of Legal Challenges to Classified Investigative Technologies. The United States Attorneys' Offices shall promptly notify the Criminal Division of any legal proceeding in which there may be potential access to, and/or disclosure of, classified investigative technologies that have been used in a criminal investigation. Thus, for example, the Criminal Division should be immediately notified of any demand or motion for the disclosure of a classified investigative technology. Similarly, if any case is being prosecuted, or considered for prosecution, in which a classified investigative technology was deployed without adherence to the procedures set forth in paragraph (A), the relevant United States Attorney's Office shall notify the Criminal Division as soon as it learns of any such deployment. The Assistant Attorney General for the Criminal Division shall supervise all litigation regarding the potential disclosure of classified investigative technologies.

(C) Exception for Emergencies Involving Imminent Danger. Notwithstanding paragraph (A), the Deputy Attorney General, the Assistant Attorney General for the Criminal Division, or any person designated by either of them, may authorize, in accordance with and to the extent permitted by applicable law and any required court process, immediate deployment of a classified investigative technology if he or she reasonably determines that an emergency involving either immediate danger of death or serious physical injury to any person or imminent harm to the national security requires deployment without delay. The Deputy Attorney General shall be promptly notified of all deployments authorized under this paragraph.

(D) Adherence to National Security Information Protocols. All Department personnel are reminded that all notifications and transmittals under this memorandum must adhere to all applicable protocols and requirements governing the transmission of National Security Information.

(E) Initial Point of Contact for Required Notifications. Agents or attorneys may initially contact the Criminal Division, as follows, in order to arrange for proper transmission of any required notifications:

Maureen H. Killion, Director
Office of Enforcement Operations
Criminal Division/DOJ
John C. Keeney Building
1301 New York Avenue, N.W.
Washington, D.C. 20530
Phone: (202) 514-6809
Fax: (202) 616-8256

(F) Construction of this Memorandum. This Memorandum is limited to improving the internal management of the Department and is not intended to, nor does it, create any right, benefit, or privilege, substantive or procedural, enforceable at law or equity, by any party against the United States, the Department of Justice, their officers or employees, or any other person or entity. Nor should this Memorandum be construed to create any right to judicial review involving the compliance or noncompliance of the United States, the Department, their officers or employees, or any other person or entity, with this Memorandum.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

JUL 10 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Please find enclosed responses to questions posed by the Committee to Deputy Attorney General Thompson and FBI Director Mueller after their testimony before the Committee on May 8, 2002 in the hearing entitled, "Reforming the FBI in the 21st Century: Reorganizing and Refocusing the Mission." We note that the Department submitted responses to questions on December 23, 2002, and April 11, 2003.

We sincerely regret the delay in responding to your important questions and recognize the need to improve our responsiveness to the Committee. Due to the number and complexity of issues involved in these responses, extensive coordination was needed amongst numerous Department of Justice components. While most answers were drafted in the fall of 2002, the nature of ongoing cases and investigations presented in many of the questions caused delay. As such, we would request that you consider these answers current as of February 2003.

Questions number one through four, submitted by Senator Leahy to FBI Director Mueller, involve the ongoing investigation into the Anthrax attacks. We anticipate that we will submit answers to the four questions soon.

Please note that responses to several questions posed to Director Mueller require the Department to provide information that is classified at the SECRET level. That classified information is being delivered to the Committee under separate cover. Also, many questions contain information that is marked as "For Official Use Only." This sensitive, but unclassified, information is noted in our attached unclassified answers, and will be delivered to the Committee under separate cover.

If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Questions Submitted by Senator Leahy
Senate Judiciary Committee Hearing on
May 8, 2002

Written Questions for Deputy Attorney General Thompson

1. **In December 2001, the FBI announced a new Office of Intelligence for strategic analysis to gather information from current and past cases and other agencies, to look for patterns and analyze risks, and to meet the needs of other organizations responsible for homeland security. At the same time, however, the Justice Department was forming a separate Foreign Terrorism Tracking Task Force outside the FBI that, according to information provided by the Department, plans to spend $20 million this year for its own intelligence analysis projects, databases, and lookout list. A Supplemental Appropriations request includes $10 million in the FBI budget to support the Task Force. If the American people hold the FBI accountable for tracking foreign terrorists, and Director Mueller briefs the President every morning with the CIA Director on terrorist threats, why shouldn't this Main Justice Task Force be part of the FBI Office of Intelligence?**

   Answer: The FBI has established interagency Joint Terrorism Task Forces in all 56 field offices. The FBI has established an interagency National Joint Terrorism Task Force (NJTTF) at FBI Headquarters.

   By memorandum dated August 6, 2002, the Attorney General ordered the Director of the FBI to "formally consolidate" the FTTTF within the Counterterrorism Division of the FBI, as part of "Phase II" of the FBI's reorganization. However, consistent with the original Presidential order creating the FTTTF, the Director of the FTTTF reports both to the Director of the FBI and to the Deputy Attorney General, which promotes coordinated information sharing with the highest levels of the Department of Justice. Congressional concurrence is being sought to move the FTTTF to the Office of Intelligence as part of an integrated plan to transform intelligence within the FBI. This move is consistent with the FBI's efforts to strengthen its entire intelligence apparatus, and will maximize a number of unique core competencies of the FTTTF. One of the FTTTF's core functions is to provide information that locates or detects the presence of known or suspected terrorists within the United States by exploiting public and proprietary data sources to find an "electronic footprint" of known and suspected terrorists. The FTTTF provides day-to-day support to the Counterterrorism Division and JTTFs in locating known and suspected terrorists and is an integral part of FBI counterterrorism operations. Hence, it is our belief that the FTTTF belongs within the Department of Justice and the FBI so that it can continue to provide direct support to counterterrorism investigations.

2. **There is apparently no secure Internet site to provide information about terrorist threats to law enforcement officials and first responders. The Justice Department**

currently has two separate systems that could use the Internet for this purpose – the FBI's Law Enforcement OnLine (LEO) and the Regional Information Sharing System (RISS) funded by the Justice Management Division. What is being done to bring these programs together so there is a unified, secure web site on the Internet for sharing terrorist threat information with state and local governments and first responders?

Answer: We are committed to sharing information and intelligence with our state and local law enforcement partners, other Federal agencies and the intelligence communities. Our goal is to collect and disseminate law enforcement and counterterrorism data quickly and effectively in order to stop terrorists before they strike.

The FBI's Law Enforcement OnLine (LEO) system provides a secure, internet-based communication system to share information with law enforcement officials and could be expanded, with additional resources, to include first responders. Similarly, the Regional Information Sharing System (RISS), which is managed by a collaborative effort of state and local law enforcement officials, provides a secure, internet-based system to share the same information but, likewise, would require expansion to include all first responders. Currently, neither system interconnects all law enforcement agencies (federal or state) and first responders.

In June 2002, representatives from FBI, RISS, and the Bureau of Justice Assistance (BJA), the Department component that partially funds the RISS program, met to discuss the need for and logistics of unifying the RISS Network (RISSNET) and LEO system. In late June 2002, the administrators of the RISS program and managers of the LEO system reached an agreement to implement a gateway to create seamless connectivity link between the two systems. The LEO and RISSNET systems were connected, with full encryption, on September 1, 2002. Technologically, a virtual private network (VPN) is initiated from current desktop and stand-alone Internet connections to achieve secure, encrypted connection and single sign-on access privileges to the connected systems simultaneously. Although both systems remain independent and continue to vett their respective users, this effort created a virtual single system for the joint users. Prior to this interface, users could not access both LEO and RISS in the same session.

Together the systems provide encrypted email across both systems, redacted databases ("pointer systems"), intelligence information, access to certain participating states' automated investigative case files, and the capability for private, invitation-only, encrypted, on-line collaboration discussions.

We are also working to improve information sharing and collaboration among public safety/public service entities. The Regional Information Sharing Systems Anti-Terrorism Information Exchange (RISS-ATIX) initiative being developed by OJP will provide a secure, unclassified intranet connection for terrorism threat communication and

information exchange with state and local first responders. We expect to have as many as 26 States connected to State Points of Contact for first responders within the next few weeks.

Finally, RISS and LEO managers have agreed to pursue plans to connect several other existing systems to RISSNET and LEO, including the National Law Enforcement Telecommunications System (NLETS), the National Crime Information Center (NCIC), and the Open Source Information System (OSIS) operated by the Intelink Program. Through OSIS, LEO and RISSNET users will be able to access the Department of State 's OpenNet Plus SBU system, and eventually the Bureau of Consular Affairs' Consolidated Consular (visa) database. The connection between LEO, RISSNET and OSIS is planned for later this spring. The other connections require additional planning and coordination.

14. **Bob Dies plans to leave the FBI on May 20th, and his successor is being recruited. In response to written questions from the Oklahoma City hearing, Mr. Dies stated that "the procurement system must be more responsive to our requirements. Much of government is risk averse and can be more concerned that all the details are attended to rather than the overall success of the program. Your continued support of an executive team trying to take prudent business risks will continue to be needed. If you expect my replacement to play by all the rules all the time very little will get done." Do you agree, and will you back up Mr. Dies' successor if he takes this approach?**

Answer: The Department of Justice will strongly support the efforts of our technology leaders to upgrade the FBI's information technology capabilities pursuant to applicable procurement laws and regulations. If appropriate, we will seek such legislative or regulatory reforms as may be necessary to expedite the modernization of the FBI's information technology systems.

17. **You testified that the Strategic Management Council's review has relied on certain aspects of an Arthur Andersen report, in addition to the report of the Webster Commission, the IG report on the Oklahoma City case, and the forthcoming IG report on the Hanssen case. The Committee has received the Webster Commission report and the first IG report and expects to receive the IG report on the Hanssen case. Please provide a copy of the Arthur Andersen report.**

Answer: A copy of the Andersen report is attached for your review.

FBI Responses to Questions Submitted by Senator Patrick J. Leahy
Following the Senate Judiciary Committee Hearing on
May 8, 2002

FBI Activities Before 9/11 Attacks

Leahy 4.*(sic)* With respect to the electronic communication dated July 10, 2001, drafted by the FBI Phoenix Field Office regarding suspicious training at U.S. aviation schools:

Answer (a) - (o) : The FBI provided an appropriately redacted version of the Phoenix document to the Committee on June 4, 2002. The document remains classified.

The FBI Office of Professional Responsibility referred the issues raised by the Phoenix EC to the Department of Justice Office of the Inspector General (OIG) on September 28, 2001. On May 21, 2002, the OIG provided its preliminary report on the handling of the Phoenix EC to the FBI and to the Joint Intelligence Committee conducting an inquiry into the events of September 11, 2001. On May 23, 2002, Director Mueller referred to the OIG the matters contained in the letter from Minneapolis Special Agent Coleen Rowley, including all aspects of the Phoenix EC. We respectfully decline to respond to matters relating to the handling of the Phoenix EC prior to completion of the reviews by the OIG and the Joint Intelligence Committee.

(p) What is the meaning of each of the various abbreviations, acronyms and code numbers used throughout the EC?

Answer: The answer to this question is classified SECRET and will be transmitted to the Committee under separate cover.

(q) Was the document marked "routine" and if so, should it have been handled in a "routine" manner?

Answer: The "Routine" precedence designation is used when addressee(s) must have the information in the normal course of business [Manual of Investigative Operations and Guidelines, Part 2, Section 16-1.4 (2)(d)]. The document was handled as routine because it was designated "routine" by the Phoenix Division.

Leahy 5. The press has reported that Filipino authorities alerted the FBI as early as 1995 that at least one of the Middle Eastern pilots who trained at American flight schools had proposed hijacking a commercial jet and crashing it into federal buildings. The pilot, Abdul Hakim Murad, was reported to have attended two flight schools - Coastal Aviation of New Bern, North Carolina, and Richmor Aviation of Schenectady, New York - in the early 1990s, and FBI Agents were reported to have visited those schools to obtain information

about Arab pilots in 1996. Is this report substantially correct? If so --

(a)-(c) Questions relating to documents in the FBI's possession before the 9/11 attacks that pertain to these matters.

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(d) Explain how information on these matters was disseminated, analyzed, and used by the FBI and, to the FBI's knowledge, by other agencies.

Answer: The Joint Intelligence Committee staff is reviewing this matter and we defer to their independent assessment.

(e) Was the information considered by the FBI when it was investigating Moussaoui or determining whether to seek a FISA search authority on Moussaoui before 9/11?

Answer: We respectfully decline to comment on this matter at this time due to the pending prosecution of Zacarias Moussaoui.

(F) Explain whether the information in the EC could have been relevant to prevention of the 9/11 attacks.

Answer: We are uncertain of the document referenced in the question and cannot speculate as to relevancy of the document in preventing the 9/11 attacks.

Leahy 6. FBI Deputy Executive Assistant Director Caruso testified on October 3, 2001, "Media reports also contend that the FBI had advance warnings since 1995 of the plot to hijack U.S. airliners. The FBI had no warnings about any hijack plots. There was a widely publicized 1995 conspiracy in the Philippines to remotely blow up 11 airliners over the Pacific Ocean but that plot was disrupted. As is the practice, the information obtained during that investigation was widely disseminated, even internationally, and thoroughly analyzed by multiple agencies. It does not connect to the current case." Did the information obtained during that investigation include any reference to the proposal to hijack a commercial jet and crash it into federal buildings?

Answer: According to debriefings provided by the Philippine National Police (PNP), during discussions with Ramzi Yousef, Abdul Hakim Murad claims to have proposed the idea of renting a small plane, loading it with explosives and flying it into CIA Headquarters. Murad also claims to have discussed the possibility of boarding a U.S. commercial airplane posing as an ordinary

passenger, hijacking it at gunpoint, gaining control of the cockpit and forcing it to crash into CIA Headquarters as a suicide mission. At one point Yousef also described a "plot" (to a third person) to build an airstrip in Afghanistan, hijack a U.S. airliner, kill the passengers, fill the plane with explosives and then fly it back to the US, where the explosives would be detonated over a major city. These plots were all discussed "in theory" and there was no evidence of any concrete plans ever being made and no evidence that they ever discussed any secondary targets (e.g., skyscrapers, the White House, the Pentagon).

Leahy 7. **The press has reported that Federal Aviation Administrator Jane Garvey stated at a news conference on September 24, 2001, "No one could imagine someone being willing to commit suicide, being willing to use an airline as a lethal weapon."**

(a) **If the FBI had information about the proposal to hijack a commercial jet and crash it into federal buildings, was it disseminated to the FAA? If it was not disseminated, please explain why not.**

Answer: The information set forth in response to Question 6 (above) was disseminated to the FAA via a CIA memo dated 2/1/95 and an FBI teletype dated 4/14/95.

(b) **Would knowledge of such a previous proposal by a Middle Eastern pilot to hijack a commercial jet and crash it into federal buildings have made it easier to imagine someone being willing to commit suicide by using an airline as a lethal weapon?**

Answer: We defer to the FAA for response.

Leahy 8. **The press reported that law enforcement officials were aware that fewer than a dozen people with links to bin Laden had attended U.S. flight schools.**

Answer: We respectfully decline to comment on this matter at this time due to the pending prosecution of Zacarias Moussaoui.

Leahy 9. **The press has reported that, in 1998, FBI agents questioned officials from Airman Flight School in Norman, Oklahoma, about Ihab Ali Nawawi who was later identified in court testimony as a pilot for bin Laden. The flight school's director of operations was quoted as saying that Nawai obtained his commercial pilot's license from Airman in the early 1990s.**

Answer: We respectfully decline to comment on this matter at this time due to the pending

prosecution of Zacarias Moussaoui.

Leahy 10. The press has reported that the trial of bin Laden associates for the 1998 bombings of U.S. embassies in Kenya and Tanzania yielded documents containing several references to flight schools and bin Laden plots.

Answer: During the investigation in the East African embassy bombings, the FBI participated in the execution of a search warrant of the office of the non-governmental organization Mercy International Relief Agency (MIRA). Among the items recovered during that search were personal documents, phone/address books and other papers belonging to Wadih el Hage. Among el Hage's documents, the FBI did obtain paper work relating to flight training for Ihab Mohammed Ali and L'Houssaine Kerchtou as well as a phone number for the Airman Flight School in Norman, Oklahoma.

Leahy 11. The press has reported that, during the trial referred to in question 10, one government witness, Essam al-Ridi, reportedly testified he had taken classes and taught at the now-defunct Ed Boardman Aviation School in Forth Worth and in the mid 1990's purchased a used Saber-40 aircraft on bin Laden's behalf for $210,000 in Tucson.

Answer: Essam al-Ridi was a government witness in the referenced trial and his entire testimony is a matter of public record in the trial transcripts. Al-Ridi testified that he attended the Ed Boardman Flight School from 1979 to 1981 and eventually did become an instructor at the same school. Al-Ridi did purchase an old T-39 military aircraft, which is similar to a civilian aircraft called a Saber-40. He purchased the aircraft for $210,000 in 1993 and was a Permanent Resident Alien of the U.S. at the time. Al-Ridi testified that he did purchase the plane on behalf of bin Laden. The plane was purchased through a dealer in Tucson, Arizona. After the purchase, Al-Ridi flew this plane all the way to Khartoum, Sudan (making a number of maintenance and refueling stops along the way). In late 1994, in Khartoum, al-Ridi was practicing flying maneuvers in this plane, with Ihab Mohammed Ali acting as co-pilot, and crashed the plane on an airfield in Khartoum due to a hydraulic problem. The plane was never fixed and is still in an embankment at the airfield in Khartoum.

Leahy 12. The press has reported that, during the trial referred to in question 10, another witness, L'Houssaine Kerchtou, testified that he was sent to a flight school in Nairobi and later served as a pilot for bin Laden.

Answer: L'Houssaine Kerchtou was a government witness in the referenced trial and his entire testimony is a matter of public record in the trial transcripts. Kerchtou testified that he attended CMC flight school training in Nairobi, Kenya and this training was funded by Al-Qaeda.

However, Kerchtou never passed his pilot's exam (failing multiple times). As such he never became a pilot.

Leahy 13. **The press has reported that Ihab Mohammed Ali, who was taken into custody in May 1999 due to his role in the Al-Qaeda network and the 1998 bombings of U.S. embassies in Kenya and Tanzania and was subsequently indicted for lying to the grand jury, took flight lessons in Oklahoma in 1993 at the Airman Flight School.**

Answer: Ihab Mohammed Ali was born in Egypt and came to the U.S. when he was three years old. He grew up in Brooklyn, NY and became a naturalized U.S. citizen. He speaks fluent English. He eventually moved to Florida and for a time worked at Disney World. Documents belonging to Wadih el Hage found during the search of MIRA (referenced in answer to question 10 above) detail an address for Ihab Ali in Norman, Oklahoma. In 1993 he did attend Airman Flight School in Norman Oklahoma.

Leahy 14. **The press has reported that the issue of how U.S. authorities processed early warning signs that terrorists were taking advantage of the flight school system would be examined in the aftermath of the attack. Suzanne E. Spaulding, executive director of the National Commission on Terrorism, a congressionally appointed task force, was quoted as stating, "In hindsight, we can see how all these things [flight school connections] might be relevant and important. But it is harder on a day-to-day basis. There is no question that technology could help sort information." What is your response to this assessment?**

Answer: Both the Department of Justice Inspector General and the Joint Intelligence Committee inquiry are reviewing pre-9/11 information regarding flight training by terrorists. In the meantime, I am restructuring and reshaping the FBI to include putting in place the analytical and information sharing capabilities needed in the post-9/11 environment. A component of these capabilities is the information infrastructure necessary to enhance our ability to collect, store, search, retrieve, analyze and share information. Prior testimony before Congress has described the problems the FBI is experiencing because of outdated technology. Thanks to support from Congress, the FBI has embarked on the information infrastructure revitalization that will enhance our mission of preventing another terrorist attack.

Leahy 15. **You testified that prior to the 9/11 attacks, the CIA gave the FBI the names of two individuals and said they had been at a meeting in Kuala Lumpur with known terrorists. They turned out to be two of the 9/11 hijackers. When the FBI tried to find them before 9/11, they had come through**

Immigration and were said to be staying at the Marriott in New York City. You stated that this information did the FBI no good and that there was no mechanism to try to identify those persons if they were stopped by police. When Attorney General Ashcroft testified last October, he said there was no procedure for putting such names on a watch list for the airlines.

(a) Is there such a procedure today and, if so, how does it work?

Answer: There is a procedure today for putting the names of potential terrorists on a watch list for the airlines. The Transportation Security Administration (TSA) maintains a No Fly List and a Selectee List to ensure that persons on whom there is sufficient intelligence information to be considered "dangerous" and whom the TSA believes could pose a threat to aviation do not fly aboard commercial aircraft, or to ensure that persons on whom there is less information, but who may be dangerous, receive additional security attention during the screening process. The FBI provides names to the TSA via a TSA detailee to FBI headquarters. The specific criteria for placing names on the TSA lists is Law Enforcement Sensitive. The FBI provides as much identifying information as possible to the TSA about each person placed on the No Fly and Selectee lists. The FBI also provides to the TSA the results of interviews with passengers and, if a match is made, recommendations as to whether or not that individual should remain on a list. However, TSA ultimately decides how to use that information, i.e., retain or remove a name from a list.

(b)-(d) Questions relating to documents in the FBI's possession before the 9/11 attacks that pertain to these two individuals.

Answer: Responsive documents are classified and consist, in whole or in part, of third agency material. We note, however, that the FBI provided the Committee a classified briefing on 2/14/02 regarding the FBI's knowledge of, and efforts to locate, these two individuals.

(e) Explain whether, in the FBI's view, the CIA could have provided the information to the FBI earlier.

Answer: The Joint Intelligence Committee staff has invested a significant amount of time on this matter and we defer to their independent assessment.

(f) What additional steps could the FBI have taken if the CIA had provided the information to the FBI earlier?

Answer: The Joint Intelligence Committee staff has invested a significant amount of time on this matter and we defer to their independent assessment.

(g) What was the FBI's role before 9/11 in collecting, receiving, analyzing, and acting upon information regarding this meeting in Kuala Lumpur

and related matters?

Answer: The answer to this question is classified SECRET and will be transmitted to the Committee under separate cover.

(h) Explain why the FBI did not place information regarding these two individuals in the National Crime Information Center file on suspected terrorist group members.

Answer: The answer to this question is classified SECRET and will be transmitted to the Committee under separate cover.

Leahy 16. With respect to the investigation of Zacarias Moussaoui before the 9/11 attacks -

(a) Provide a narrative account of all activities by or known to the FBI related to the investigation and a narrative account of such activities suitable to be made public.

Answer: We respectfully decline to respond at this time due to the pending prosecution of Zacarias Moussaoui. We note, however, that the FBI provided a classified briefing on this matter to the Committee on 2/14/02.

(b) Provide a list of all documents in the FBI's possession before the 9/11 attacks that pertain to this matter.

Answer: See response to 16(a).

(c) Make those documents available for review.

Answer: See response to 16(a).

(d) Provide copies of all those documents that may be made public, in redacted form if necessary.

Answer: See response to 16(a).

Leahy 17. The following questions are based on press reporting of the Moussaoui investigation before the 9/11 attacks, and responses should provide information in the possession of the FBI before 9/11. Information obtained after 9/11 should be identified as such and provided only as needed to

understand or assess the importance of information in the FBI's possession before 9/11.

(a) Initial Report

Answer: Attached is a letter dated December 26, 2001 from Timothy J. Nelson of the Pan Am Flight School to the FBI which responds to each of the Committee's questions in this regard.

(b) Investigation - Moussaoui Interviews and Search

Answer: We respectfully decline to comment on this matter at this time due to the pending prosecution of Zacarias Moussaoui. We note, however, that the FBI provided a classified briefing on this matter to the Committee on 2/14/02.

(c) Investigation - Pan Am Flight School

Answer: See response to 17(b).

(d) Investigation - Foreign National Contacts in Oklahoma

Answer: See response to 17(b).

(e) Investigation - Oklahoma Flight School

Answer: See response to 17(b).

(f) Investigation - FBI Source Queries

Answer: See response to 17(b).

(g) Foreign Intelligence and Foreign Government Information

Answer: See response to 17(b).

(h) Alleged Plan for Deportation to France

(1) **Answer**: Consideration was being given to deportation of Moussaoui at the time of the September 11, 2001 attacks.

(2) **Answer**: See response to 17(b).

(i) HQ Analysis of Terrorists and Flight Training

Answer: See response to 17(b).

(j) **FISA Search Issue:**

1. **Did FBI investigators in Minneapolis want to seek a criminal search warrant to inspect the laptop?**

Answer: Yes.

2. **During internal discussions at the FBI from Aug. 18 to 20, did officials at headquarters oppose the request, arguing that investigators could not show probable cause that a crime had been committed?**

Answer: When information was presented to FBIHQ by agents of the Minneapolis field office, it was clear that Moussaoui's behavior was suspicious, but we were told of no facts that would indicate criminal activity that could have served as a predicate to obtain a criminal search warrant. Accordingly, FBIHQ advised the field agents that they had not yet demonstrated the probable cause necessary to seek a criminal search warrant. FBIHQ also directed the Minneapolis field agents to confer with their Chief Division Counsel.

3. **Did the FBI counsel in the Minneapolis office concur, arguing that the U.S. attorney's office there would be unlikely to grant approval?**

Answer: Information available at FBIHQ indicates that the Minneapolis Chief Division Counsel advised that they lacked probable cause necessary to satisfy the U.S. Attorney that a criminal search warrant was justified.

4. **Did the proposed FISA application include a classified cable in August from the French intelligence service saying that Moussaoui had radical Islamic beliefs and identifying a friend as having fought in Chechnya with an Algerian Muslim group that included a known bin Laden associate?**

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

5. **Did the French information tie Moussaoui directly to al Qaeda or any other terrorist group?**

Answer: The answer to this question is classified SECRET and will be

transmitted to the Committee under separate cover.

6. **Was this information considered as part of a decision that there was not sufficient probable cause to obtain a warrant under the FISA statute?**

Answer: The answer to this question is classified SECRET and will be transmitted to the Committee under separate cover.

7. **Was a problem in obtaining FISA authority that investigators had no reliable evidence that Moussaoui was connected to any group designated a terrorist organization by the State Department?**

Answer: No. Whether a terrorist organization has been designated as such by the Department of State is irrelevant to the need to satisfy the statutory requirement that a person is an agent of a foreign power.

8. **Did the concern about Moussaoui reach, as the press reports, "the top echelons of the FBI, prompting a flurry of unusual meetings between agents and bureau lawyers trying to secure a special intelligence warrant?"**

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

9. **On Aug. 23, did the FBI receive a lead from France, where intelligence officials said he had been linked to a young man who had died fighting alongside anti-Russian Islamic rebels in Chechnya?**

Answer: The answer to this question is classified SECRET and will be transmitted to the Committee under separate cover.

10. **Did the French say the dead man's family blamed Moussaoui for radicalizing their son?**

Answer: The answer to this question is classified SECRET and will be transmitted to the Committee under separate cover.

11. **Did the United States transmit photos of Moussaoui to the French for display to the dead man's family?**

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

12. Is it correct that U.S. officials suspect the Chechen rebel group had a relationship with bin Laden and the Taliban militia in Afghanistan, but it is not designated as a terrorist organization, so that Moussaoui's connection to it could not form the basis for an intelligence warrant? Even if it had, did FBI lawyers say it was doubtful that Moussaoui's casual connection to one of its alleged fighters would lead to a FISA warrant?

Answer: Parts of the answer to this question are classified SECRET and marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

13. Did the reluctance to seek a warrant coincide with a secret internal investigation prompted by Royce C. Lamberth, the chief judge of the Foreign Intelligence Surveilllance Court, which issues the warrant, about past FBI requests for them?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

14. Did that review limit the ability to seek wiretaps on Moussaoui?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

15. Would a FISA search have produced any information indicating the use of flight schools or aircraft for terrorist purposes?

Answer: We respectfully decline to comment; the subsequent search of Moussaoui's computer remains part of the pending criminal case.

16. Is it correct that the search uncovered a commercially available flight simulation program, information about wind currents, jetliners and crop-dusting airplanes?

Answer: See response to 17(j)(7).

17. Do FBI and Justice Department officials believe that the information in Moussaoui's possession would have provided few tangible clues for investigators at the time?

Answer: See response to 17(j)(7).

18. Did the focus on FISA search application prevent or distract from consideration of other measures, such as warning FAA and airlines or contacting other flight schools.

Answer: No.

Leahy 18. Since 9/11 you have identified the need for FBI improvements including information management and computer systems, analytic capability, counterterrorism and prevention, additional translators and Agents with foreign language skills. New information keeps coming to light, such as the Phoenix office recommendation on flight schools. As you reorganize the FBI, what is being done to take a systematic look at the lessons of the FBI's pre-9/11 performance?

Answer: Both the Joint Intelligence Committees and the Department of Justice Inspector General are taking comprehensive, systematic looks at the FBI's handling of pre-9/11 information. I look forward to their recommendations and have asked the Inspector General to provide interim recommendations even before his review is completed.

In the meantime, I have taken various steps to deal with problems or issues already brought to light. For example, the handling of the Phoenix memorandum revealed issues concerning both the review and dissemination of such documents (both within the FBI and with other agencies) and the new structures in the Counterterrorism Division, including the substantially enhanced analytical structure and a National Joint Terrorism Task Force, should improve the FBI's performance in both of these critical areas, as should the new mechanisms for sharing information with the CIA.

Similarly, the Moussaoui matter has demonstrated issues concerning the handling of FISAs. New procedures designed to ensure appropriate high level review of FISAs - up to and including myself - should improve performance in this area as well.

Various other reforms already under way deal with other aspects of what we have already learned from our review of pre-9/11 performance, and we are confident we will learn additional lessons from the ongoing Inspector General and Joint Intelligence Committee reviews.

Leahy 19. **This Committee needs to be kept informed of what you discover about FBI activities before 9/11 that might have been relevant to the attacks. Much of that information is still classified, including information about what the FBI did in the Moussaoui case and aspects of the case of the two hijackers whose names were given to the FBI before the attacks. Do you agree to brief the Committee on these matters in a closed session?**

Answer: The FBI has briefed the Committee on these matters in closed session.

Leahy 20. **In December 2001 you created a new position of Executive Assistant Director for Counterterrorism/Counterintelligence to supervise a new Office of Intelligence, and you abolished the Investigative Services Division where the FBI's terrorism analysts were located. Those actions reversed a 1999 reorganization that split the FBI's counterterrorism program between two Assistant Directors. What was wrong with the 1999 decisions, and why did you create a new management structure for FBI counterterrorism?**

Answer: The creation of the four new Executive Assistant Directors - including one for Counterterrorism and Counterintelligence - was not an undoing of the 1999 decision to split counterterrorism and counterintelligence. The two Divisions remain separate, and both are being enhanced.

The reasons for changes in the Counterterrorism Division structure are to effectuate the new overriding priority of prevention of terrorism through a national control and focus for the program, substantially enhanced analytical capacity, improved mechanisms for coordination with other agencies and with state and local law enforcement, and better programmatic focus and control, among other things.

The abolition of the Investigative Services Division does reflect a change from the decision made in 1999. Based on input from many people within the FBI, I believed that the experience with the ISD since 1999 had not been successful and that it made more sense to locate analysts within the substantive Divisions of their subject matter expertise.

Leahy 21. **In December 2001 the FBI announced a new Office of Intelligence for strategic analysis to gather information from current and past cases and other agencies, to look for patterns and analyze risks, and to meet the needs of other organizations responsible for homeland security. At the same time, however, the Justice Department was forming a separate Foreign Terrorism Tracking Task Force outside the FBI that, according to information provided by the Department, plans to spend $20 million this year for its own intelligence analysis projects, databases, and lookout list. A Supplemental Appropriations request includes $10 million in the FBI budget to support the**

Task Force. If the American people hold the FBI accountable for tracking foreign terrorists, and you brief the President every morning with the CIA Director on terrorist threats, why shouldn't this Main Justice Task Force be part of the FBI Office of Intelligence?

Answer: The FBI has established interagency Joint Terrorism Task Forces in all 56 field offices. The FBI has established an interagency National Joint Terrorism Task Force (NJTTF) at FBI Headquarters.

By memorandum dated August 6, 2002, the Attorney General ordered the Director of the FBI to "formally consolidate" the FTTTF within the Counterterrorism Division of the FBI, as part of "Phase II" of the FBI's reorganization. However, consistent with the original Presidential order creating the FTTTF, the Director of the FTTTF reports both to the Director of the FBI and to the Deputy Attorney General, which promotes coordinated information sharing with the highest levels of the Department of Justice. Congressional concurrence is being sought to move the FTTTF to the Office of Intelligence as part of an integrated plan to transform intelligence within the FBI. This move is consistent with the FBI's efforts to strengthen its entire intelligence apparatus, and will maximize a number of unique core competencies of the FTTTF. One of the FTTTF's core functions is to provide information that locates or detects the presence of known or suspected terrorists within the United States by exploiting public and proprietary data sources to find an "electronic footprint" of known and suspected terrorists. The FTTTF provides day-to-day support to the Counterterrorism Division and JTTFs in locating known and suspected terrorists and is an integral part of FBI counterterrorism operations. Hence, it is our belief that the FTTTF belongs within the Department of Justice and the FBI so that it can continue to provide direct support to counterterrorism investigations.

Leahy 22. Your statement makes the point, which I agree with, that the FBI's new Office of Intelligence is very important for strategic analysis to meet counterterrorism and counterintelligence needs. Why, then, more than five months after its creation was announced, has no one been found to head the new Office?

Answer: I recently announced the appointment of Mark Miller, a CIA employee and expert in the field, to head the new intelligence effort. It took longer than I would have liked to find the right person, but Mr. Miller is now on board and working aggressively to improve the FBI's performance in this critical area.

Leahy 23. After the mail box attacks on May 2-4, 2002, one of the best places to inform the American people was the Internet. I am concerned that neither the FBI, the Postal Service, or the Homeland Security Office used the Internet very effectively. At noon on Monday, May 6, for example, the FBI's public Internet home page had the text of a letter that accompanied the mail box

devices, but no link to the Postal Service web site. The Postal Service advisory on its web site was dated Saturday and did not mention the May 4 bombings in Nebraska. The Homeland Security Office web site had nothing relevant at all. The press reported new advisories, but the Government was not using the one method of communication that millions of Americans - on farms and in cities - rely on for basic information in their daily lives. What are you doing to make the Internet a more valuable resource for the American people in times of terrorist threats like this?

Answer: We agree with the Committee that the Internet is an excellent tool for effectively and efficiently disseminating information to the public. We have reviewed the archives of the FBI's website for this time period and found that, as of May 6, 2002, the FBI offered not only the text of the letter that accompanied the devices, but also hyperlinks to both the U.S. Postal Inspection Service and the Bureau of Alcohol, Tobacco and Firearms. We will continue to utilize the Internet as a resource in our counterterrorism efforts.

Leahy 24. **There does not appear to be a secure Internet site to provide information about terrorist threats to law enforcement officials and first responders. The Justice Department currently has two separate systems that could use the Internet for this purpose -- the FBI's Law Enforcement OnLine (LEO) and the Regional Information Sharing System (RISS) funded by the Justice Management Division. What is being done to bring these programs together so there is a unified, secure web site on the Internet for sharing terrorist threat information with state and local governments and first responders?**

Answer: We are committed to sharing information and intelligence with our state and local law enforcement partners, other Federal agencies and the intelligence communities. Our goal is to collect and disseminate law enforcement and counterterrorism data quickly and effectively in order to stop terrorists before they strike.

The FBI's Law Enforcement OnLine (LEO) system provides a secure, internet-based communication system to share information with law enforcement officials and could be expanded, with additional resources, to include first responders. Similarly, the Regional Information Sharing System (RISS), which is managed by a collaborative effort of state and local law enforcement officials, provides a secure, internet-based system to share the same information but, likewise, would require expansion to include all first responders. Currently, neither system interconnects all law enforcement agencies (federal or state) and first responders.

In June 2002, representatives from FBI, RISS, and the Bureau of Justice Assistance (BJA), the Department component that partially funds the RISS program, met to discuss the need for and logistics of unifying the RISS Network (RISSNET) and LEO system. In late June 2002, the administrators of the RISS program and managers of the LEO system reached an agreement to implement a gateway to create seamless connectivity link between the two systems. The LEO

and RISSNET systems were connected, with full encryption, on September 1, 2002. Technologically, a virtual private network (VPN) is initiated from current desktop and stand-alone Internet connections to achieve secure, encrypted connection and single sign-on access privileges to the connected systems simultaneously. Although both systems remain independent and continue to vett their respective users, this effort created a virtual single system for the joint users. Prior to this interface, users could not access both LEO and RISS in the same session.

Together the systems provide encrypted email across both systems, redacted databases ("pointer systems"), intelligence information, access to certain participating states' automated investigative case files, and the capability for private, invitation-only, encrypted, on-line collaboration discussions.

We are also working to improve information sharing and collaboration among public safety/public service entities. The Regional Information Sharing Systems Anti-Terrorism Information Exchange (RISS-ATIX) initiative being developed by OJP will provide a secure, unclassified intranet connection for terrorism threat communication and information exchange with state and local first responders. We expect to have as many as 26 States connected to State Points of Contact for first responders within the next few weeks.

Finally, RISS and LEO managers have agreed to pursue plans to connect several other existing systems to RISSNET and LEO, including the National Law Enforcement Telecommunications System (NLETS), the National Crime Information Center (NCIC), and the Open Source Information System (OSIS) operated by the Intelink Program. Through OSIS, LEO and RISSNET users will be able to access the Department of State 's OpenNet Plus SBU system, and eventually the Bureau of Consular Affairs' Consolidated Consular (visa) database. The connection between LEO, RISSNET and OSIS is planned for later this spring. The other connections require additional planning and coordination.

Leahy 25. Last year, the Justice Department announced that it was reviewing the Attorney General's guidelines for FBI investigations and investigative techniques to determine whether changes were needed to deal with the terrorist threat. There are reports, for example, that the guidelines for handling informants are being revised.

(a) Has the FBI had any problem operating under the Attorney General's Guidelines since 9/11? If so, please explain.

Answer: At the direction of the Attorney General, the FBI and various components of the Department of Justice reviewed certain sets of Attorney General Guidelines in the aftermath of the terrorist attacks of September 11, to identify and revise provisions in those guidelines which could unduly impede the FBI's counterterrorism and law enforcement missions. The revised

guidelines were issued by the Attorney General on May 30, 2002.

(b) What is the FBI's position on any proposals to change those guidelines?

Answer: The FBI believes that certain provisions of the previous guidelines, some of which were promulgated many years ago, could at times unduly impede our operations. The FBI and the Department complied with the Attorney General's directive, by identifying and proposing appropriate revisions to such provisions with a view toward preserving the guidelines' key safeguards.

(c) Will Judiciary Committee Members have an opportunity to comment on any changes that are seriously considered?

Answer: Prior to their publication, changes to the Guidelines were briefed to the Committee.

Leahy 26. The FBI has stated that the new Terrorism Watch List ("TWL") will include names of individuals "of investigative interest to the FBI" and names "provided by the Intelligence Community and cooperating foreign governments." You testified that names would be placed on the TWL if the FBI was interested in talking to individuals to obtain information from them, even if they are not suspected of terrorist activity. You stated that the FBI has various "gradations" on the watch list, depending on the threat and whether there is any paper outstanding for the individual. It is not clear how those categories fit the criteria that currently govern the placement of names in the FBI's National Crime Information Center, and there is concern that the TWL may include individuals holding dissident political or religious views with no legitimate connection to terrorism. With resepct to the TWL:

(a) What are the criteria and procedures being used to place names on the FBI Terrorism Watch List, including any safeguard to prevent misuse and procedures to implement those safeguards?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(b) Please explain the "gradations" and how they affect the use of the list.

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(c) If the list includes people who are not wanted for any crime or for any

immigration violation, what do you expect the local police to do if they pull over such a person?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(d) Is the FBI reconsidering or revising existing guidelines for the NCIC? If so, what changes are being considered?

Answer: Yes, the FBI is revising existing guidelines for the NCIC to add sub-groups for categories of persons who may not meet the criteria for existing NCIC files.

Leahy 27. You testified that the FBI has a 24-hour watch to receive telephone calls from airline security to help determine whether, if someone's name comes up on a list, he or she is actually the person the FBI intends for airline security to stop. You also stated that other agencies may put names on the watch list. Is an interagency mechanism needed to determine whether, if a person's name is on the watch list, he or she is actually the person another agency intends to track or stop?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

Leahy 28. During our oversight hearings last summer, Ray Kelly, former Commissioner of Customs and now New York City Police Commissioner, recommended a regional structure so field offices could not become too independent. Since then, we have learned that some FBI field offices failed to share terrorism information with others in the Bureau who had a need to know. The immediate reaction last October was to order all offices to share everything with everybody on the FBI's internal computer system, and the Webster Commission came down hard on that action because it exposed sensitive FISA information too widely. What should be done to bring field offices under control so that there is a unified FBI to combat terrorism?

Answer: The FBI's information technology is being replaced to enhance our ability to access, organize and analyze information. Specifically, the Trilogy Program will migrate five investigative applications into a "Virtual Case File" (VCF), to provide user-friendly, web browser access to mission critical information. A web-based interface will enable FBI employees to have a graphical interface with investigative information. It will eliminate the cumbersome aspects of our current system, greatly enhance our collaborative environment and go a long way towards eliminating the problems identified by the Webster Commission and the DOJ Inspector General.

Leahy 29. **Are you satisfied that everything possible is being done to bring sensitive FISA information that was loaded on the FBI's computer system under need-to-know access controls?**

Answer: Yes. Today, certain case types are automatically restricted when they are created. The FBI's Security Division is currently facilitating a review of whether additional types of cases should be restricted. Representatives from the FBI operational divisions are intimately involved in this review. Headquarters and field components may currently request that access restrictions be placed on specific case information and may also audit access attempts using a reporting utility within the Automated Case Support (ACS) system. At the beginning of June 2002, a new web-based tool will be deployed to drastically simplify and improve the case audit process. Specific policies and procedures are being prepared to support the deployment of this tool, called the Case Document Access Report (CDAR). They will contain step-by-step instructions for restricting case access and for using the CDAR. They will be disseminated Bureau-wide. An awareness effort, directed to both FBI Headquarters and field office personnel concerning the handling and use of sensitive case information, to include FISA-derived information, is also being developed.

Leahy 30. **You testified that the FBIHQ Counterterrorism Division "must not just coordinate but direct and manage investigations in the future." I would like your reaction, as a former U.S. Attorney, to this trend to centralize control over criminal cases, including terrorism cases, at the Department. For instance, we have heard that local FBI field offices have been directed in some cases not to share information directly with the federal prosecutor down the street from them, but instead to send it to Washington first, and let Washington send it back to the U.S. Attorney. Is that happening? Based on your past experience do you think that is wise?**

Answer: There is always some tension between centralized direction and control and local autonomy. The changes being made in counterterrorism at the FBI do not reflect a general trend towards centralization of control over criminal cases - to the contrary, my expectation is to continue and even enhance local control over criminal cases other than in the counterterrorism and counterintelligence areas. In those two areas, the nature of the threat dictates national control. In general, there is no reason why information should have to be sent to Washington before being shared with a local U.S. Attorney's office, although in some cases the particularly sensitive nature of certain information may require treating it in this manner. There has been no general directive that counterterrorism information has to be sent to Washington before being

shared with a U.S. Attorney's office.

Leahy 31. **Your testimony cited three new programmatic tools for the FBI Counterterrorism Program: the Financial Review Group, the telephone applications group and new data mining capabilities. Please describe each of the tools and how they are coordinated with similar efforts by other federal agencies.**

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

Leahy 32. **As a former prosecutor, one thing that used to be very frustrating to me was the law enforcement obsession with "stats." While statistics are an important measurement tool, I have also found that sometimes it leads individual agents or even whole agencies to focus too much on the quantity of cases as opposed to the quality of cases. That is why one provision of S. 1974, for which Senator Grassley has provided important leadership, asks for a GAO report on the collection and use of such statistics by federal agencies. Based on your experience, do you agree that this is a serious problem and, if so, what is being done to correct it?**

Answer: There can be a problem with over reliance on statistics, especially if it is done to the exclusion of a qualitative analysis of the impact of a program. As we switch to prevention as our priority in counterterrorism, this potential problem becomes more acute and we are currently working to develop appropriate methods to measure our progress in this area. More generally, I am interested in developing better methods for measuring progress throughout the FBI's programs rather than the current statistics, in order to try to develop a more qualitative assessment of the success of our law enforcement efforts.

Leahy 33. **Bob Dies plans to leave the FBI on May 20th, and his successor is being recruited. In response to written questions from the Oklahoma City hearing, Mr. Dies stated that "the procurement system must be more responsive to our requirements. Much of government is risk averse and can be more concerned that all the details are attended to rather than the overall success of the program. Your continued support of an executive team trying to take prudent business risks will continue to be needed. If you expect my replacement to play by all the rules all the time, very little will get done." Do you agree, and will you back up Mr. Dies' successor if he takes this**

approach?

Answer: We will strongly support the efforts of our information management people to upgrade the FBI's technology through procurement reform if necessary and otherwise.

Leahy 34. **The FBI has to better focus its missions on the things for which we rely on it in order to address the challenges for the future. You testified that you expect to come back to Congress "in the next couple of weeks" to discuss with Members where the FBI will take resources from that are required to address terrorism. This would occur after you look at each of the programs with the help of the SACs. Please provide the results of your deliberations with the SACs regarding the programs that would have reduced resources.**

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

Leahy 35. **When you mention some priority areas of federal enforcement in your testimony, you did not include environmental crime in your list. Do you think that these matters are an important federal concern and that the FBI should play a leadership role in investigating environmental crimes that can be so important to protect the public's health and safety?**

Answer: Environmental crimes are important and the FBI will continue to devote resources to them. Indeed the current reprogramming does not take any agent resources out of environmental crime. However, any list of priorities, by definition, does not include everything an agency does and environmental crimes, while important, are not as high a priority as the matters included on this list. In part this is a recognition of the fact that the Environmental Protection Agency has a program devoted to dealing with such crimes.

Questions Submitted by Senator Russell D. Feingold Following the Senate Judiciary Committee Hearing on May 8, 2002

Feingold 1. **During the hearing, I told you about the experience of 20 Wisconsin peace activists who were stopped at the Milwaukee airport on Friday, April 19, 2002 on their way to Washington, DC. Their experience is chronicled in various news stories, including "Security fear keeps peace group at airport; Member's name resembled one on anti-terrorism list," *Milwaukee Journal Sentinel*, April 20, 2002, and, "McCarthyism Watch," *The Progressive*, April 27, 2002 .... The *Milwaukee Journal Sentinel* reports that the name of one member in the peace group resembled that of a person on a national anti-terrorism database. *The Progressive* suggests that the names of more than one person in the group triggered a possible match on the watch list. At the hearing, you said that you were unaware of this particular incident. Now that you have had an opportunity to look into this incident, please provide an explanation of what happened.**

(a) How many individuals triggered a possible match on the watch list?

Answer: One individual, Jacob T. Laden, triggered a possible match on the TSA No Fly list.

(b) Please explain why these individual(s) triggered the watch list.

Answer: Jacob T. Laden triggered the list because the single-name "Laden" appeared as the alias of an individual deemed to be dangerous and a threat to civil aviation. However, Jacob T. Laden booked a block of airline tickets. Therefore, pursuant to Security Directive 1544, all individuals booked in that party were considered No Fly individuals.

(c) Were any of these possible matches determined to be actual matches on the watch list? If so, why were these individuals on the watch list? Does the FBI suspect them of a link to or association with another terrorist group?

Answer: None of these possible matches were determined to be actual matches on the No Fly list. However, airport and law enforcement officials on the scene could not resolve all 37 potential matches before the flight had to depart in order to meet the curfew requirements in Washington D.C. Therefore, 20 individuals who missed the flight were provided meals and

lodged in a hotel at the airline's expense. All persons lodged overnight were flown to Washington, D.C. the next morning on a 7:00 a.m. flight. It is noted that three hours after the event began, airline employees were advised by TSA personnel that all individuals in the group could have been cleared to fly after the individual whose name actually appeared on the watch list was cleared. Since this event, airline personnel have been provided better training and the airline has, pursuant to new Security Directives from the TSA, developed its own initial plan for clearing passengers listed on the No Fly list. The FBI does not suspect any of the individuals in this group of a link to or an association with Al Qaeda or Al Qaeda members, nor to another terrorist group.

Feingold 2. (a) Please explain the differences among the FBI Terrorism Watch List, watch lists maintained by the Central Intelligence Agency (CIA), and the watch list maintained by the Transportation Security Administration (TSA) (hereinafter referred to as the "TSA Watch List").

Answer: The FBI Terrorism Watch List (TWL) is a law enforcement/investigative tool used either to effect an arrest, to identify and track activity of a known individual under active investigation, or to identify an unknown person and determine if further investigation is warranted. The TWL is a comprehensive list of names based on information identified through FBI and JTTF investigations, US Intelligence Community reporting, and Department of Defense intelligence gathering as well as information provided by foreign intelligence/security services. FBIHQ decides which names are placed on the TWL.

The TSA Watch Lists are an aviation security measure used either to ensure that persons on whom there is sufficient information to be classified by the TSA as dangerous and whom the TSA believes could pose a threat to aviation do not fly aboard commercial aircraft, or to ensure that persons on whom there is less information, but who may be dangerous, receive additional security attention during the screening process.

The CIA Watch Lists have an intelligence and analytical purpose, and are used to advise the FBI and other U.S. and non-U.S. government law enforcement and intelligence agencies of potential terrorists' identities and activities.

(b) What are the criteria for placing names on the FBI Terrorism Watch List?

Answer: Criteria for placing names on the FBI Watch List include pending formal criminal charges; pending terrorism investigations by the FBI; and, individuals of interest to the FBI who may not be the subjects of an active FBI investigation, but on whom further tracking and record

checks to determine potential connections to ongoing investigations appears warranted.

(c) How does the criteria used by the FBI differ from the criteria for placing names on the TSA Watch List and CIA list?

Answer: The criteria for placing names on the TSA Watch Lists centers on whether or not the person is known to be, or may be, dangerous and is known to, or may, present a threat to civil aviation, regardless of pending legal or investigative action of another agency. The criteria for the CIA list are based on intelligence and assessment of the terrorist threat to U.S. interests.

(d) How are names placed by the FBI on the FBI Terrorism Watch List shared with the TSA and CIA?

Answer: Names placed by the FBI on the FBI TWL who may present a threat to civil aviation are shared with the TSA via a full-time TSA detailee to the FBI. Assigned to the International Terrorism Operations Section, the detailee has access to incoming intelligence from field offices and other government agencies. The CIA also has full-time detailees in the International Terrorism Operations Section who have direct access to daily terrorism threat intelligence, but only indirect computer access to names on the FBI TWL.

(e) What advice does the FBI provide to TSA regarding the creation and placement of names on the TSA Watch List?

Answer: The FBI provides recommendations to the TSA regarding which names the FBI might want on the TSA Watch Lists. The FBI has, in the past, also offered advice as to a suitable minimum amount of information which might be required before someone is added to a TSA Watch List.

(f) What coordination, guidance or advice does the FBI provide to TSA regarding how to use information in the TSA Watch List?

Answer: The FBI provides as much identifying information as possible to the TSA about each person placed on the TSA No Fly and Selectee lists. The FBI also provides to the TSA the results of interviews with passengers and, if a match is made, recommendations as to whether or not that individual should remain on a list. However, TSA ultimately decides how to use that information, i.e., retain or remove a name from a list.

(g) What guidance or advice does the FBI provide to TSA regarding the detention and questioning of airline passengers who "trigger" the TSA Watch List?

Answer: The FBI has provided the TSA with guidance and advice on how law enforcement can effect a quick and thorough identification of passengers who "trigger" the No Fly or Selectee lists. The FBI advised the TSA that airport law enforcement officers, because they are more readily available "on-scene" than FBI agents, are in a better position to rapidly eliminate obvious non-matches to a listed person, and that the FBI would respond in cases where the officer was unable to determine whether or not the person on the No Fly or Selectee list and the passenger were identical. The TSA incorporated this guidance into its Security Directives. The FBI advised the TSA that it will interview, polygraph and conduct interviews of passengers who cannot otherwise be eliminated by the airport police as a "match" to a person on the No Fly or Selectee list.

(h) What is the purpose or use of each list, including the FBI Terrorism Watch List, TSA Watch List, and CIA list?

Answer: The purpose of the lists is to prevent another terrorist attack in the US, against US Citizens and US Interest; to collect, analyze, and share intelligence regarding terrorism with othe agencies; and to monitor individuals/groups of terrorist activities.

Feingold 3. At the hearing, you testified that the FBI Terrorism Watch List may contain the names of individuals who are not suspected of terrorism but who are associates of Al Qaeda members or others who engage in terrorism.

(a) How does the FBI determine whether someone is an "associate" of Al Qaeda members or others who engage in terrorism?

Answer: The FBI analyzes all available intelligence from a variety of sources to assess whether someone is an "associate" of Al Qaeda members or others who engage in terrorism.

(b) If someone simply attends the same mosque as a suspected terrorist, is that person placed on the FBI Terrorism Watch List or TSA Watch List?

Answer: No, a person is not placed on the FBI Terrorism Watch List or TSA No Fly or Selectee lists if they simply attend the same mosque as a suspected terrorist.

(c) If someone is on the mailing list for a publication that expresses dissident political or religious views and is also received by a suspected terrorist, is that person placed on the FBI Terrorism Watch

List or TSA Watch List?

Answer: No, a person is not placed on the FBI Terrorism Watch List solely because they are on the mailing list for a publication that expresses dissident political or religious views and that publication is also received by a suspected terrorist.

Feingold 4. **(a) Does the FBI Terrorism Watch List only contain the names of individuals who are suspected of links to Al Qaeda or terrorism, or individuals who are associated with individuals who are suspected of links to Al Qaeda or terrorism? If not, what other individuals are included on the FBI Terrorism Watch List?**

Answer: Yes, the FBI Terrorism Watch List only contains names of individuals who are suspected of links to Al Qaeda or other terrorism, or who are associated with individuals who are suspected of links to Al Qaeda or other terrorism.

(b) Does the TSA Watch List only contain the names of individuals who are suspected of links to Al Qaeda or terrorism, or individuals who are associated with individuals who are suspected of links to Al Qaeda or terrorism? If not, what other individuals are included on the TSA Watch List?

Answer: No, the TSA No Fly and Selectee lists also contain names of individuals who are known to be dangerous and to pose a threat to civil aviation, or who may be dangerous and may pose a threat to civil aviation, regardless of whether or not information links them to terrorism.

Feingold 5. **(a) Does the FBI Terrorism Watch List include individuals who hold dissident political or religious views but have no connection to Al Qaeda or terrorism? If yes, what kinds of dissident political or religious views would result in the FBI's determination that the individual should be placed on the FBI Terrorism Watch List?**

Answer: No, the FBI Terrorism Watch List does not contain names of individuals who hold dissident political or religious views but have no connection to Al Qaeda or terrorism. All individuals on the TWL have a connection to either Al Qaeda or to other International and Domestic Terrorist groups/individuals.

(b) Does the TSA Watch List include individuals who hold dissident

political or religious views but have no connection to Al Qaeda or terrorism? If yes, what kinds of dissident political or religious views would result in the FBI's determination that the individual should be placed on the TSA Watch List?

Answer: This question is referred to the TSA, as the FBI does not have specific information on all persons on the TSA lists. Under no circumstances does the FBI use dissident political or religious views as a criteria to determine that anyone should be placed on any list.

Feingold 6. What mechanism is available for someone who believes they have been improperly placed on the TSA Watch List to be removed from the list?

Answer: Someone who believes that they (not just their name) have been improperly placed on the TSA No Fly or Selectee lists may contact the TSA for information on how to be removed from the list. If the individual was placed on the list by the FBI, the TSA may refer that person to the FBI, in which case the FBI would attempt to resolve the matter.

Feingold 7. What guidance does the Department of Justice or the FBI provide to the Transportation Security Administration to ensure that individuals are not wrongly detained or unreasonably inconvenienced at our nation's airports?

Answer: To ensure that individuals are not wrongly detained or unreasonably inconvenienced at our nation's airports, the FBI has advised TSA to remove names from the list of persons who are incarcerated or for whom the FBI has conducted a thorough interview and determined that they do not present a threat to civil aviation.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

JUL 17 2003

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find the Department of Justice's fourth and final submission to questions posed to Deputy Attorney General Thompson and FBI Director Mueller after their appearance before the Committee on May 8, 2002. Many of these responses contain information that is labeled "For Official Use Only." This sensitive, but unclassified information, is noted in our attached answers.

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

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Leahy 1. You testified that a revision of the FBI profile of the suspect in the anthrax investigation is not warranted at this time.

(a) What impact does this profile have on the conduct or direction of the FBI's investigation?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(b) The New York Times on May 11, 2002, reported that "[t]he FBI remains convinced that the attacks were carried out by an American with scientific training, not by Al Qaeda or a rogue nation, but critics fear the bureau is so wedded to this theory that it has become blind to other possibilities." How do you respond to this criticism?

Answer: The FBI has not precluded any category of suspect, motive or theory. While we are using a number of investigative support techniques, such as criminal profiling, which have proved helpful in other cases, the evidence drives this case, and investigators will follow it wherever it goes.

Leahy 2. The New York Times reported, on May 6 (sic), 2002, that the anthrax sent to me (Leahy) was "the deadliest of all." Again, the New York Times reported, on May 11, 2002, that the "Leahy letter, mailed the same day as the Daschle letter, contained an even finer, highly volatile powder in which the anthrax spores were more uniformly small and dangerous."

(a) Is it correct that the FBI has not been able to test the anthrax sent to Senator Daschle, because the sample is too small, or the anthrax that killed Bob Stevens in Florida, so the FBI does not know for sure which anthrax letter was the most deadly?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(b) Has the FBI been able to determine any difference between the anthrax sent to me (Leahy) and to Senator Daschle and, if so, what are those differences and explanations for them?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(c) Has the FBI been able to determine any differences between the anthrax sent

to me (Leahy) and to the New York Post and, if so, what are those differences and explanations for them?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

(d) Has the FBI been able to determine any differences between the anthrax sent to me (Leahy) and that which killed Bob Stevens in Florida, if so, what are those differences and explanations for them?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

Leahy 3. Tests conducted on the anthrax sent to me (Leahy) apparently show a silicon layer incorporated in the spores, which is significantly different from the anthrax sent to the New York Post. What effect, if any, of the silicon and why would someone add silicon to the anthrax?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

Leahy 4. The Washington Post, on May 9, 2002, reported that the anthrax sent through the mail "are direct descendants of the germs developed at Fort Detrick, according to scientists who did the work." Under the supervision of the FBI, laboratories are now comparing samples of the anthrax sent through the mail with anthrax samples collected from labs around the country in order to pinpoint the exact source of the spores. How much of this comparison has been completed to date and how long do you estimate this process will take before all the comparison tests are completed?

Answer: The answer to this question is marked For Official Use Only (FOUO) and will be transmitted to the Committee under separate cover.

SUBMISSIONS FOR THE RECORD

Statement of
The Honorable Orrin Hatch
United States Senator
Utah

May 8, 2002

PRINTABLE VERSION

Mr. Chairman, I would like to start off by welcoming Deputy Attorney General Thompson and Director Mueller, and thanking them both for taking the time to appear before us here today.

Those of us who have been intimately involved in the war on terrorism are well-acquainted with the remarkable service that these two gentlemen have provided to this country since September 11th. However, there may be people present in the hearing room, or watching these proceedings on C-Span, who are not closely acquainted with the inner workings of the Justice Department or the FBI.

To those people, I simply wish to say that there are no two individuals in the federal government who have worked more tirelessly, or more effectively, to help to ensure that the events of September 11th will never be replicated.

In the days immediately following September 11th, as the enormity of what had occurred began to sink in, I think it is safe to say that many of us wondered if our lives would ever be the same - if we would ever be able to regain some semblance of normality.

Many people around the world predicted that America's reaction would be to turn inward - that we would become a closed and defensive society.

It is now clear, that those predictions have not come to pass. Make no mistake, we have not forgotten the events of September 11th, and we maintain our unshakeable resolve to undertake any sacrifice that will be required to bring to justice those who are responsible.

But the terrorists have not succeeded in changing our daily way of life. We remain the world's most open, most free society. Our civil liberties have not been eroded in any meaningful fashion. With the exception of those heroic members of our armed forces who have been mobilized and sent overseas to confront this threat, the greatest inconvenience most of us face in our daily lives is longer waits at metal detectors before boarding an airplane or entering a government building.

At the same time, we have regained a large measure of the security we felt prior to the events of September 11th. True, we no longer bask in the naive notion that we are immune from terrorist attack on American soil. But our naivety has been

replaced, not with fear, but with a healthy and appropriate sense of alert.
In my opinion, the response of the Department of Justice and the FBI to the September 11th attacks has, in large measure, been responsible for our success in regaining our sense of security without the sacrifice of our precious civil liberties.

Since September 11th, the Justice Department and the FBI have moved in a thoughtful, measured fashion to improve the capacity of our law enforcement institutions to detect and prevent terrorist activity. They requested appropriate tools from the Congress, with which to fight terrorism - tools that were largely provided by Congress with the passage of the Patriot Act. Director Mueller, in coordination with the Justice Department, also moved on self-initiative, as he promised at his confirmation hearing, with appropriate Congressional consultation, to reorganize the FBI to devote a greater share of their resources to anti-terrorist activities, and to cooperate with other segments of the federal government, and with local and state law enforcement agencies, participating in the war on terrorism.

Our law enforcement institutions have emerged from this crisis more efficient, more focused, and more effective.

Attorney General Ashcroft set the tone of the DOJ's response not long after the September 11th attacks when he said that the Department can no longer afford to be all things to all people. Instead, he said, the lives of our citizens will depend on the Department doing fewer things, but doing those things exceptionally well.

I believe the Department and the FBI have risen to the challenge laid down by the Attorney General. I am amazed, in particular, that Director Mueller has been able to accomplish such wide-ranging reforms within the FBI, given the fact that, during his entire tenure as Director, he has been charged with leading the response to the September 11th attacks.

I am confident that the FBI and the Department of Justice are moving in the right direction. I look forward to hearing the testimony from the witnesses today, and to continuing to work with the Department and the Bureau to assist them in their essential mission of protecting our citizens from harm.
####

- TOP OF THIS PAGE
- RETURN TO HOME

PRINTER FRIENDLY VERSION

U.S. SENATOR PATRICK LEAHY

CONTACT: David Carle, 202-224-3693 VERMONT

STATEMENT OF SENATOR PATRICK LEAHY,
CHAIRMAN, SENATE JUDICIARY COMMITTEE
FBI REFORM SERIES
HEARING ON
"REFORMING THE FBI IN THE 21ST CENTURY:
REORGANIZING AND REFOCUSING THE MISSION"
MAY 8, 2002

This hearing marks the continuation of the Judiciary Committee's series of bipartisan FBI oversight hearings that began last summer. We have considered the report of former Senator John Danforth on the Waco confrontation, the Webster Commission report on FBI security in the wake of the Hanssen espionage case, and the Justice Department Inspector General's report on the belated disclosure of FBI documents in the Oklahoma City bombing case. We have heard the important perspectives of FBI agents and senior officials about what they believe the FBI must do to address morale and accountability problems, and to improve the Bureau's security and counterespionage programs, computer systems, and information management practices. The Members of this Committee have paid close attention and on April 25, voted unanimously to report to the full Senate for consideration, the FBI Reform Act of 2002, S. 1974.

The risk of catastrophic terrorism – as we know so vividly from the 9/11 and anthrax attacks – has made amply clear that nothing is more critical to the safety of the American people than a well-organized and skillfully managed FBI that uses its power and resources effectively while adhering to the Constitution and the rule of law. The FBI has two key and overlapping missions: protecting our national security by rooting out spies and terrorists, and protecting our public safety by investigating criminal activity. Today's hearing looks at how the FBI can reorganize and refocus its efforts to perform both missions with the resources made available by the President and the Congress.

Pre-Sept. 11 Issues: In my view, you cannot plan for the future effectively without knowing what went wrong in the past. Before we can learn any lessons from recent experience, we need to develop the lesson plan by examining what happened. In devising a new counterterrorism strategy for the FBI to prevent future terrorist attacks, we need to determine whether any institutional flaws in the FBI impaired the government's ability to prevent the 9/11 attacks. That is why I wrote to the Attorney General on October 25, 2001, requesting that relevant material be preserved, and on November 8, 2001, I recommended asking Judge Webster's Commission to review the FBI's pre-9/11 performance. While the Attorney General did not commission an outside review, this Committee has an obligation to understand the lessons of the 9/11 attacks for

reorganizing the FBI and refocusing its mission.

This grave duty can only be discharged by the Committee responsible for oversight of the entire Bureau – its national security functions, its other law enforcement tasks, and the support structure within which both are performed. When Judge Webster came before us to describe the deficiencies in FBI security that allowed Robert Hanssen to spy for the Russians undetected for more than 20 years, he described the "institutional" vulnerabilities of the FBI as "shocking" and "devastating"– this from a former FBI and CIA Director. Likewise, when the Justice Department Inspector General told us that "widespread failures by the FBI" led to the belated disclosure of documents in the Oklahoma City bombing case, the FBI's current Executive Assistant Director for Administration, Bob Chiradio, testified that the Director had made the IG's report "recommended reading for all FBI management and supervisory personnel."

In each case the FBI's knee-jerk response *before* those reports came out was to minimize its responsibility. The American public was told Hanssen was 'too smart to get caught.' The American people were told that computers, not people, caused the delay in the production of documents in the Oklahoma City case. Yet, the Webster Commission and IG reports made clear that FBI security flaws enabled Hanssen's spying, and that bad judgment as well as computers contributed to the production delays in the Oklahoma City case. Indeed, in both cases it was more than that – a major participating cause was the deeply imbedded culture of the FBI.

Today we are still in the same position regarding the 9/11 attacks as we were before the Webster Commission and IG reports. The American people are being told that the conspirators were too clever to have been caught. We are being told that the hijackers avoided detection because they combined meticulous planning and extraordinary secrecy with discipline, fanaticism and extensive knowledge of how America works. We hear that nothing short of a member of the inner circle turning himself in would have provided sufficient foresight to have prevented the attacks.

Those explanations may indeed be correct. No one would blame the American public, however, for wanting to examine those explanations. There may be more to the 9/11 story than the skill of the enemy – just as there was more to the story of Hanssen than his intellect and more to the story of the Oklahoma City documents than computers. When senior FBI officials concede in testimony before this Committee that the FBI does not know all that it knows, we are left to wonder whether the FBI effectively used relevant information that it knew before the watershed events on 9/11.

Continuing press reports allege the FBI failed to pursue pre-9/11 leads effectively, including warnings about two hijackers and, just last week, a report of concerns of the FBI's Phoenix office about the possibility of terrorists at U.S. flight schools a few months before the 9/11 attacks. The FBI provided to the Committee a single paragraph from the otherwise classified Phoenix report that states:

> "Phoenix believes that the FBI should accumulate a listing of civil aviation universities/colleges around the country. FBI field offices with these types of

> schools in their area should establish appropriate liaison. FBIHQ should discuss this matter with other elements of the U.S. intelligence community and task the community for any information that supports Phoenix's suspicions. FBIHQ should consider seeking the necessary authority to obtain visa information from the USDOS on individuals obtaining visas to attend these types of schools and notify the appropriate FBI field office when these individuals are scheduled to arrive in their area of responsibility."

I hope that the Director will help us get to the bottom of this incident, including finding out exactly what was said in the FBI report, to whom it was sent, and whether any action was taken in response to that FBI report.

Other provocative questions also need to be pursued. Shortly before the 9/11 attacks, the FBI reportedly was notified that an individual who had met with individuals implicated in the bombing of the USS Cole had entered the United States with an associate. The FBI began to search for these men, but did not find them before they hijacked the plane that flew into the Pentagon. When Attorney General Ashcroft testified last October, I asked if there was a procedure for putting such names on a watch list for the airlines. He said there was not. The next questions, of course, are "Why not?" and "Is there now such a procedure?" Other questions are what steps did the FBI take to find the two men, and how long did it take to enlist other agencies in the search? If the names had been placed on an airline watch list, or the FBI had the information earlier, would it have increased the chances of disrupting at least part of the attack?

Here are some things we already know about FBI operations that potentially limited out nation's defenses against terrorism before 9/11:

– The Bureau's **information management and computer systems were so flawed** that the FBI had no real way to know what information it had in its possession.

– Some **FBI field offices operated so independently** that their information was not shared with other parts of the Bureau that needed it, let alone with other agencies.

– In 1999 the **leadership of the FBI's counterterrorism program had been split** between two divisions, with terrorism analysts placed under an Investigative Services Division manager with little national security or intelligence community experience.

– The FBI **lacked the strategic analysis capability** to gather information from current and past cases, reach out for information from other agencies, look for patterns, analyze risks, plan strategy for its own operations, and meet the needs of organizations responsible for security measures.

– The FBI had **no comprehensive terrorism watch list** to bring together the names of all suspected foreign terrorists known to the FBI and other federal agencies.

– The FBI **did not put any names of terrorist group members in the National Crime**

Information Center file that was designed years earlier to provide information about suspected terrorists to other federal, state, and local law enforcement agencies.

– The FBI **lacked the translators and the Agents with foreign language skills** necessary to develop sources, conduct effective interviews, read foreign documents, and monitor electronic surveillance in international terrorism cases.

The American people and the U.S. Congress should not be hearing about information such as the Phoenix memorandum as it is periodically leaked to or uncovered by the media. The American people deserve a full accounting of this matter.

Senator Hatch and I have made a joint request for additional funding to examine the events leading up to the September 11 attacks and what steps are needed to make sure that our law enforcement is in a position not to let history repeat itself. That request has been blocked by Minority Leader Lott. An examination of FBI operations before 9/11 are essential, not to lay blame, but to learn lessons and to be in a position to evaluate the FBI reorganization plans.

I look forward to discussing with the Deputy Attorney General and Director Mueller the reasons for the reorganization and other management actions they have underway. The Director has already restored unity of command under a new Executive Assistant Director for Counterterrorism/Counterintelligence, sought to strengthen FBI analysis by creating an Office of Intelligence, posted the identities of terrorist group members on the NCIC, and ordered the development of a comprehensive Terrorism Watch List to serve the law enforcement and intelligence communities. These are all important steps.

At the same time, I am concerned about new management issues that directly affect the FBI's counterterrorism role. For example, the Department appears to be developing two counterterrorism intelligence organizations – an **FBI Office of Intelligence** that brings together terrorism information from other agencies and other countries for a comprehensive FBI Terrorism Watch List and a separate **Main Justice Foreign Terrorist Tracking Task Force** that reports to the Deputy Attorney General. This new Main Justice Task Force plans to spend nearly $20 million for its own intelligence analysis projects, databases, and lookout list. Why is this Task Force reporting to the Deputy Attorney General, rather than to the FBI Director, who has the daily responsibility alongside the CIA Director to brief the President on terrorist threats? Would the best course be to make the Task Force mission and assets a vital part of the new FBI Office of Intelligence?

Another example, is the Justice Department's maintenance of two separate systems for using the Internet to share information among law enforcement agencies and first responders – the **FBI's Law Enforcement OnLine (LEO)** and the **Justice Management Division's Regional Information Sharing System (RISS)**. Has the time come to bring these programs together to meet the requirement for a unified, secure Internet system for sharing critical homeland security information with first responders?

Our nation's counterterrorism and homeland security efforts are too important to allow these

organizational issues to remain unresolved.

Criminal Investigation Issues: Turning to the FBI's other criminal investigative work, the Committee needs to consider the preliminary ideas of the Director and the Deputy Attorney General for de-emphasizing certain FBI missions. On March 6, Director Mueller said that the FBI is "developing a comprehensive strategy to permanently shift resources to the fight against terrorism and in support of a massive prevention effort."

The FBI cannot be all things to all people. Too often our first response to any new and important law enforcement problem has been to assign the problem to the FBI.. Too many carjackings? Too much domestic violence? Too much simple drug possession? Too many drive-by shootings? The answer has long been to create federal penalties and put the FBI on it. Over and over again, whenever the nation has faced a new or emerging crime problem, America has turned to the FBI to solve it, even though we have other fine Federal, State and local police and investigative agencies fully capable of addressing such problems.

It is a testament to the overall confidence we have in the FBI that we turn to the Bureau so reflexively, but the FBI cannot be as effective at focusing on problems that only the FBI can handle when the attention of field agents is constantly diverted to problems that are important, but can be handled by other agencies.

I know the Director is confronting hard decisions about how to refocus the FBI's mission and reorganize the Bureau, and this Committee may ask tough questions about the decisions he makes. But if recent history has taught us anything, it is that asking the tough questions is in the best interest of the American people.

# # # # #

Statement of FBI Director Robert S. Mueller
Senate Committee on the Judiciary
May 8, 2002

The FBI faces daunting challenges from an increasingly volatile world situation. Terrorists at home and abroad threaten U.S. interests at unprecedented levels. Foreign intelligence services continue to target U.S. secrets and technology, often for their own countries' economic advantage. Cyber-space is threatened by increasingly malicious criminal activities. Organized crime of all types operates without regard to geographic borders. And most obvious, the tragic events of September 11th have changed the American landscape forever.

Responding to these challenges requires a redesigned and refocused FBI, imperatives reinforced by the recent findings of Inspector General Fine and Judge Webster. We must refocus our missions and priorities. New technologies must be put in place to support new and different operational practices. And, we must improve how we hire, manage and train our workforce; collaborate with others; and manage, analyze, share and protect information. All will be necessary if we are to successfully evolve post-9/11. Most would have been necessary even absent 9/11.

I believe that we all recognize that given the scope and pace of needed change, that the FBI is in a period of transformation. This transition is not only organizational and technological, but also cultural. I am more impatient than most but we must do these things right, not simply fast. Refashioning a large organization takes not only a reformer's zeal, but also a craftsman's patience. But

the task of transforming the Bureau is a national priority and well worth the large expenditure of effort by all of us involved.

Nevertheless, despite the large scope of the challenge, I believe we are making progress on all fronts and I very much appreciate your recent comments Chairman Leahy when you said, "The men and women of the FBI are performing the task with great professionalism at home and abroad. Americans have felt safer as a result of the full mobilization of the FBI's dedicated Special Agents, its expert support personnel, and its exceptional technical capabilities" because our people are our greatest asset.

Change has many dimensions. We are not only structurally different, but we are fundamentally changing our approach in a number of areas, most notably counter-terrorism, counter-intelligence and technology. As this Committee knows, many of these initiatives are works in progress, with final decisions still to come. Currently, I am working closely with Deputy Attorney General Thompson, the Attorney General's Strategic Management Counsel and our own executives on all of these issues and I anticipate being in a position to discuss them in depth in the coming weeks. I am also meeting with our Special Agents in Charge for the third time next week to consult with them as we continue to work through the complex issues inherent in remaking the FBI.

Central to any successful structural change at the FBI is new technology. As this Committee knows from prior hearings, our information infrastructure is far

behind current technology. It cannot support the robust analytical capacity we need. Fortunately, Congress has provided us substantial funding and we are deploying new hardware and networks on an accelerated schedule. But, having to so dramatically replace the entire infrastructure rather than make incremental improvements, as is common in the private sector, makes the replacement process more difficult. I am continuing to bring in extremely talented individuals to assist in this endeavor and will keep the Congress regularly advised about both the progress we make and the difficulties we encounter.

Just as we change our technology, we must reshape and retrain our workforce. Over the years the FBI tended to hire generalists, operating within a culture that most jobs were best done by Agents. Former Director Freeh began changing that notion. We are accelerating this approach. We are hiring subject matter experts in areas like IT, foreign languages, internal security, area studies, engineering, records and the like.

There also has been much in the media about coordination with state and municipal authorities, what is commonly referred to as information sharing. After a series of meetings with our law enforcement colleagues and state homeland security directors, it became clear that our history of solid, personal relationships alone was not addressing the basic information needs of our counterparts. They have our

attention and we are doing much better. Adding 650,000 state and local officers to our efforts is the only way to make this truly a national effort, not just a federal effort.

To move forward on this broad range of issues, we took a significant step in the process of change with a major reorganization of the FBI. The first phase of our comprehensive plan established four new Executive Assistant Directors who report directly to me and oversee key areas of our work: Counterterrorism and Counterintelligence; Criminal Investigations; Law Enforcement Services; and Administration. This structure reduced the span of control of the former Deputy Director position, a management concern raised here on Capitol Hill and in internal and external reviews of the Bureau. These changes also increased accountability and strengthened executive-level management oversight of day-to-day operations, and permitted a greater focus on strategic management issues.

The reorganization addressed other significant issues as well. It created a stand-alone Security Division, headed by an experienced professional from the CIA who has appeared before this Committee, to raise our security practices and standards to the level we need to remedy the weaknesses that the Hanssen investigation made painfully obvious. It also included a Records Management Division, led by an experienced records expert who also has appeared before this Committee, to help us modernize our record-keeping systems, policies, and processes to ensure there is no repeat of the OKBOMB document situation. It

established an Office of Law Enforcement Coordination that will not only improve relationships and information sharing with state and local police professionals and others, but will also help the FBI tap into the strengths and capabilities of our partners. We are hiring High Point, North Carolina Police Chief Louis Quijas, an experienced executive from local law enforcement to head this new office. He is someone who will better integrate our state and municipal counterparts in the war against terrorism and into major criminal investigations.

At the same time, the ongoing reorganization responds directly to the events of September 11 by putting a coordinating analytic umbrella over Counterterrorism and Counterintelligence. The new structure creates the Office of Intelligence, which will focus on building a strategic analysis capability and improving our capacity to gather, analyze, and share critical national security information, an initiative supported by our new College of Analytical Studies at Quantico. It also creates a new Cyber Division dedicated to preventing and responding to high tech and computer crimes, which terrorists around the world are increasingly exploiting to attack America and its allies. Our old approach was fractured and not well coordinated. The new Cyber Division will move elements of the Criminal Investigative Division and National Infrastructure Protection Center (NIPC) into one coordinated entity. This change will bring together various cyber initiatives and programs so we are better focused, organized, and coordinated in working with our public and private sector partners to protect our Nation's growing digital

marketplace and electronic infrastructure.

We are now in the second phase of our reorganization. As part of this phase, we are developing a comprehensive strategy to permanently shift resources to supplement the substantial new resources Congress has already provided in the fight against terrorism and in support of a massive prevention effort. Given the gravity of the current terrorist threat to the United States, the FBI must make the hard decisions to focus its available energies and resources on preventing additional terrorist acts and protecting our Nation's security. At the same time, I want to assure you that we will continue to pursue and combat international and national organized crime groups and enterprises, civil rights violations, major white-collar crime, and serious violent crime consistent with the available resources and the capabilities of, and in consultation with, our federal, state, and municipal partners.

We believe the changes to date and those that will be proposed in the near future are vital to ensuring that the FBI effectively satisfies its national security, prevention and criminal investigative missions. They represent important steps in the difficult process of change. But what emerged from the events of 9/11 leaves no doubt about the need or urgency for change.

Our massive investigation of 9/11 paints a sobering portrait of the 19 hijackers and makes clear they carried out their attacks with meticulous planning, extraordinary secrecy, and extensive knowledge of how America works.

The plans were hatched and financed overseas, beginning at least five years

ago, but perhaps going back even further. Each of the hijackers came from abroad: 15 from Saudi Arabia, two from the United Arab Emirates, and one each from Lebanon and Egypt. All 19 entered our country legally, and only three had overstayed the legal limits of their visas on the day of the attacks.

While here, the hijackers did all they could to stay below our radar. They contacted no known terrorist sympathizers. They committed no egregious crimes. They blended into the woodwork.

The hijackers also apparently left no paper trail. In our investigation, we have not yet uncovered a single piece of paper -- either here in the U.S. or in the treasure trove of information that has turned up in Afghanistan and elsewhere -- that mentioned any aspect of the September 11th plot. As best we can determine, the actual hijackers had no computers, no laptops, no storage media of any kind. They used hundreds of different pay phones and cell phones, often with prepaid calling cards that are extremely difficult to trace. And they made sure that all the money sent to them to fund their attacks was wired in small amounts to avoid detection.

In short, the terrorists managed to exploit loopholes and vulnerabilities in our systems, to stay out of sight, and to not let anyone know what they were up to beyond a very closed circle. The patient, skilled and exploitive approach used by the hijackers means our prevention efforts must be massive, globally collaborative and

supported by ample technology and analytical capacity. It means that the information possessed by every agency - - both here and abroad, both federal and local - - must go into the multi-agency prevention mix and be acted upon.

In response to 9-11, and with an eye towards preventing future attacks, the Bureau has strengthened ties with the Central Intelligence Agency, placing key staff in each others' command centers. In addition, we are members of the Foreign Terrorist Tracking Tack Force, and are expanding the number of Joint Terrorism Task Forces, which include other federal agencies and state and municipal officials. Within the FBI we have centralized accountability within the Counter Terrorism program under a new Assistant Director. Among the new programmatic tools at his disposal will be the Financial Review Group to focus on disrupting the flow of financial resources to terrorists, the Telephone Applications group, and new data mining capabilities.

But foremost among the lessons I think we have learned in retrospect is the need for substantially greater and more centralized analytic capability resident at headquarters but available anywhere in the world to all who are combating terrorism. We need a capacity with ample resources, better technology and better training, one that is better intertwined with other agencies - - domestic and foreign, federal and local - - and all the information they may possess. We are designing our new counterterrorism program and technology, standing up an Office of Intelligence, changing our training at Quantico, and hiring subject matter expertise with that

exact premise in mind. The capacity must be in place to permit every piece of information from every source to be rapidly evaluated from an analytical perspective.

It is also important, as we search for ways to improve our Nation's capacity to prevent terrorism, for America to put the attacks of 9-11 in context. The terrorists took advantage of America's strengths and used them against us. They took advantage of the freedoms we accord to our citizens and guests, particularly freedom of movement and freedom of privacy. And as long as we continue to treasure our freedoms, we always will run some risk of future attacks.

In addition, the terrorists also took advantage of the openness of our society. 50 million people, Americans and guests, entered and left America during the month of August 2001, the month preceding the 9-11 attack. The vastness of this number highlights the dynamic openness of our society. It is also the source of our economic strength and vitality. But this openness does bring with it vulnerabilities, as 9-11 so terrifyingly showed. America will continue to be free and open, and we at the FBI believe that our job is to protect these freedoms, not reduce them in the cause of security. However, these attacks highlight the need for a different FBI, more focused, more technologically adept, more reliant on outside expertise, and better equipped to process and use the vast quantities of information available to us.

I and the 27,000 women and men of the Bureau, were devastated by the attacks and remain deeply affected. But with this has come the conviction to do everything within our power to reduce the risks that Americans run in the exercise

of their freedoms. It is to this goal that all the reorganization, reform, technology and new personnel are committed. But ultimately, standing behind all the capabilities that we have now and that we are working to build is a cadre of FBI professionals, men and women who exemplify courage, integrity, respect for the law, and respect for others. I am extremely proud of how they have performed over the past eight months. As Chairman Leahy recently recognized, they have worked long days and nights, sacrificing time with their families to get the job done. It is an honor to appear before this Committee representing them.

STATEMENT OF

LARRY D. THOMPSON

DEPUTY ATTORNEY GENERAL

BEFORE THE COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

MAY 8, 2002

Chairman Leahy, Senator Hatch, Members of the Committee, thank you for inviting me to appear today to review our progress in strengthening the Federal Bureau of Investigation. This task is among our preeminent and most urgent missions at the Department of Justice because of the FBI's central role in preventing and disrupting terrorist attacks against our homeland. The Department's success in this effort is critical to restoring the full confidence of the American people in the FBI and to enabling the FBI to fulfill its counter-terrorism mission – and its many other important missions – with distinction.

On June 20, 2001, the Attorney General directed the Justice Department's Strategic Management Council to conduct a comprehensive review of the FBI and to make recommendations for reforms. The Strategic Management Council is a group that I chair, composed of senior Justice Department officials, including the FBI Director and heads of other major Justice Department agencies.

The Attorney General gave three specific directions in performing this review:

- First, he directed that a private consulting firm be hired to conduct a management study of the FBI, with particular attention to the issues of information technology, personnel management, crisis management, and performance appraisal.

- Second, the Attorney General directed that a wide array of views be solicited from individuals and organizations within and outside the Justice Department, including Congress.

- Third, the Attorney General directed that we take into account three other reviews then under way: (1) the Webster Commission's review of the FBI's internal security practices in the wake of the Hanssen espionage matter; (2) the Inspector General's (IG's) investigation of that same matter; and (3) the IG's study of the FBI's document handling procedures in the Oklahoma City bombing case.

As directed, the Department retained a management consulting firm last July to conduct this review. The consultants conducted an extensive analysis of the Bureau, including interviews with a wide variety of FBI personnel and a thorough examination of the FBI's information technology infrastructure. The consultants then submitted a report for consideration by the Strategic Management Council.

To fulfill the Attorney General's directive to solicit a wide range of informed opinion, my staff and I conducted informal interviews with a broad cross-section of individuals, including, among others:

- former Attorneys General and Deputy Attorneys General;
- former FBI Directors and Deputy Directors;
- Members of Congress and their staffs;
- leaders of organizations representing state and local law enforcement authorities;
- heads of other federal law enforcement agencies; and
- current senior Justice Department officials, including a number of United States Attorneys.

In addition, we have carefully examined the Inspector General's final report concerning the belated production of documents in the Oklahoma City bombing case, as well as the report of the Commission for the Review of FBI Security Programs, chaired by Judge William Webster. We anticipate receiving the Inspector General's report concerning the Hanssen case in the next few months, and have already received preliminary comments from the IG's office regarding FBI internal security practices.

Although we began work on this project immediately following the Attorney General's directive in July 2001, the terrorist attacks of September 11, 2001, changed both our timing and our perspective. Those attacks brought into immediate focus the need to intensify our counter-

terrorism efforts and accord an even higher priority at the FBI to the counter-terrorism mission. Moreover, the attack caused us to shift our focus from investigating crimes with an eye to prosecution, to detecting, preventing and disrupting terrorists' plans.

We are now in the process of developing specific recommendations. That process is still under way, however. We have not yet formalized our recommendations to the Attorney General.

While Director Mueller already has initiated improvements at the Bureau in a broad range of areas, I would particularly like to commend him for the measures that the FBI has instituted to strengthen its counter-terrorism capabilities.

- The FBI has already initiated significant management changes, establishing four new Executive Assistant Directors who report to the Director, one of whom has specific responsibility for Counterterrorism and Counterintelligence.
- The FBI's Joint Terrorism Task Forces have been expanded to 47 field offices and, by August 2002, will be operating in all 56 FBI field offices. The JTTF's have effectively merged the resources of a constellation of federal, state and local law enforcement agencies through cooperative information sharing.
- Making use of the USA PATRIOT Act's provisions expanding information sharing, the FBI now communicates more efficiently and successfully in disseminating critical time-sensitive information about the threat of terrorist attacks to state and local law enforcement, as well as other federal agencies.

For example:

- The FBI's NCIC database, accessible by 650,000 state and local law enforcement officers throughout the United States, has been expanded to include the names and identifying information of subjects of domestic and foreign terrorism investigations.
- The FBI is expediting security clearances for appropriate state & local law enforcement officials.

- The FBI has established a new Office of Law Enforcement Coordination to institutionalize information sharing and coordination with state and local law enforcement.
- The FBI also has recently established a College of Analytical Studies and an Office of Intelligence, and has committed to hiring more than 100 intelligence analysts to enhance its ability to gather, analyze and share national security information.

The FBI also plays an integral role in the new National Security Coordination Committee (NSCC), which I chair. The Department inaugurated the NSCC in March 2002 in order better to coordinate policy, planning and operations, and more efficiently allocate resources in our paramount mission to prevent, defeat and disrupt terrorist attacks before they occur.
The other members of the NSCC include:

- The Director of the FBI – with the participation of the Executive Assistant Director for Counter-Terrorism/Counter-Intelligence;

- The Commissioner of the Immigration and Naturalization Service;
- The Chief of Staff to the Attorney General;
- The Assistant Attorney General of the Criminal Division – with the participation of the Terrorism and Violent Crime Section, the Office of International Affairs and other components;
- The Assistant Attorney General for the Office of Justice Programs; and
- The Counsel of the Office of Intelligence and Policy Review.

This new structure is helping us to marshal our wide-ranging resources to develop, direct and execute our counter-terrorism strategy and to eliminate terrorist threats before they develop into terrorist acts. The FBI's central role in the NSCC dovetails with our overall effort to integrate the FBI's counter-terrorism functions with those of other components within the Department and with the entire intelligence and law enforcement communities.

In addition, the FBI has already begun to take steps to enhance its internal security procedures and modernize its information technology infrastructure.

Once we have completed our review, we will forward our recommendations to the Attorney General. We look forward to continue working together with this Committee to sustain the FBI as our bulwark in the defense of our freedom. This will be a detailed and demanding task – requiring a dedication to persevere long beyond September's flush of fury and grief. We at the Department of Justice are committed to this effort – not only to begin it, but to follow

through and achieve our goal and the goal of Director Mueller to restore the FBI to its proper place as the nation's preeminent law enforcement agency. Accomplishing this objective is clearly in our national interest.

Mr. Chairman, Senator Hatch, and other Members of the Committee, that completes my prepared remarks. I would be pleased to respond to your questions at this time.

STATEMENT BY SENATOR STROM THURMOND (R-SC) BEFORE THE SENATE JUDICIARY COMMITTEE, REGARDING FBI OVERSIGHT, WEDNESDAY, MAY 8, 2002, SD-106, 2:00 PM.

Mr. Chairman:

Thank you for holding this hearing regarding the mission of the FBI in the 21st Century. In the wake of the attacks of September 11, it is particularly appropriate that we refocus FBI operations on the prevention of terrorism. As the Bureau shifts its emphasis and resources accordingly, I believe that it should withdraw from areas of law enforcement that are better handled by other Federal agencies and state and local governments. It is far better for the Bureau to perform fewer duties well than to spread itself thin as a result of too many responsibilities.

The FBI is the primary agency responsible for enforcing Federal criminal statutes. Over the years, the FBI has become involved in narcotics, bank robberies, and child support enforcement, principally due to the federalization of many crimes. The Bureau's involvement in drug enforcement was also strengthened in the 1980s when Attorney General William F. Smith placed the Drug Enforcement Administration (DEA) under the policy guidance of the FBI.

While the expansion of FBI duties was well-intentioned,

the result has been an unnecessary intrusion into areas better policed by other agencies and state governments. The Commission on the Advancement of Federal Law Enforcement, established by the Anti-Terrorism and Effective Death Penalty Act of 1996 and chaired by William Webster, reported in January 2000 that Congress should restrain from federal "intrusion" into the affairs of state and local governments. The continued federalization of crime not only pushes states out of legitimate law enforcement efforts, but also results in the FBI extending itself too far, hampering its ability to function efficiently.

Due to the national security needs that the FBI must address, it is time that we considered pulling the Bureau out of areas such as narcotics enforcement. This would eliminate intrusion into local affairs, while allowing the Bureau to focus intently on fighting terrorism. As a result, the FBI would function more effectively in its antiterrorism efforts, and, in keeping with federalism principles, we would return to the states the ability to prosecute local crimes.

In addition, as the FBI re-examines its duties and responsibilities, I hope that this Committee will encourage

greater information sharing between Federal and state law enforcement. It is critically important that local communities receive information necessary to respond to potential terrorist threats. In this regard, the Regional Information Sharing System (RISS) is an excellent tool for the exchange of information between law enforcement officers, and we should encourage its further development and use.

RISS is a secure network that allows law enforcement to share criminal intelligence information. It is accessed by nearly 6,000 local, state, and Federal law enforcement agencies and is crucial to thousands of investigations. RISS is itself composed of six regional intelligence centers, allowing local needs to be met but at the same time feeding into a national system. The Regional Organized Crime Information Center (ROCIC) encompasses my home state of South Carolina, and it has been invaluable to the state's law enforcement officers.

It is important to note that the USA PATRIOT Act expanded RISS to allow for the sharing of information relating to "multi-jurisdictional terrorist conspiracies and activities." Therefore, Congress has made the determination

that information related to terrorism investigations should be used by local law enforcement. Given the renewed focus of the FBI on the prevention of terrorism, it is entirely appropriate that important information be shared with state and local law enforcement via RISS.

It has come to my attention that the FBI operates a Law Enforcement Online (LEO) program that functions in similar ways to RISS, and there has been some discussion about integrating the two systems. I am interested in considering any proposals that ensure the continued relevance and significance of RISS, but would also allow for a more coordinated Federal-state approach to preventing acts of terrorism.

Mr. Chairman, I appreciate your interest in the renewed focus of the FBI. I welcome Deputy Attorney General Larry Thompson and FBI Director Robert Mueller here today, and I look forward to hearing their testimony. Through continued mutual efforts, I have confidence that we can fashion a new and improved direction for the FBI in the 21st Century.

○